



# **NAVAL POSTGRADUATE SCHOOL**

**MONTEREY, CALIFORNIA**

## **THESIS**

**GSM NETWORK EMPLOYMENT  
ON A MAN-PORTABLE UAS**

by

Darren J. Rogers

September 2012

Thesis Co-Advisors:

Raymond R. Buettner  
Kevin D. Jones

**Approved for public release; distribution is unlimited**

THIS PAGE INTENTIONALLY LEFT BLANK

<b>REPORT DOCUMENTATION PAGE</b>			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.				
<b>1. AGENCY USE ONLY (Leave blank)</b>		<b>2. REPORT DATE</b> September 2012	<b>3. REPORT TYPE AND DATES COVERED</b> Master's Thesis	
<b>4. TITLE AND SUBTITLE</b> GSM Network Employment on a Man-Portable UAS			<b>5. FUNDING NUMBERS</b>	
<b>6. AUTHOR(S)</b> Darren J. Rogers				
<b>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</b> Naval Postgraduate School Monterey, CA 93943-5000			<b>8. PERFORMING ORGANIZATION REPORT NUMBER</b>	
<b>9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)</b> N/A			<b>10. SPONSORING/MONITORING AGENCY REPORT NUMBER</b>	
<b>11. SUPPLEMENTARY NOTES</b> The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number <u>N/A</u> .				
<b>12a. DISTRIBUTION / AVAILABILITY STATEMENT</b> Approved for public release; distribution is unlimited			<b>12b. DISTRIBUTION CODE</b>	
<b>13. ABSTRACT (maximum 200 words)</b>  <p>There are numerous national systems that offer communications support with enhanced capabilities to support ISR. For the tactical unit, it can be challenging and cumbersome to deal with national systems that may or may not be able to provide near real-time support due to other, high priority tasking. The deployment of a low-cost GSM communications support system with enhanced capabilities (CSSEC) to support intelligence, surveillance and reconnaissance (ISR), which a tactical unit could have organically, would relieve the warfighter of having to depend on national assets and processes. Employing a CSSEC system on a man-portable or small UAS would allow the range of the system to be greatly extended, as opposed to a ground-based system which may be difficult to operate in a high-threat environment.</p> <p>Commercial off-the-shelf (COTS) hardware is readily available and easily acquired. With a CSSEC deployed on a UAS, a tactical unit conducting ground operations would not be geographically constrained to a specific location to conduct ISR. Nor would they draw attention to the unit in having to set up antennas and other equipment on a building or outpost.</p> <p>Leveraging COTS hardware and open-source software will keep overall cost low without having to deal with software licensing requirements associated with proprietary systems.</p>				
<b>14. SUBJECT TERMS</b> Unmanned Aerial Systems, OpenBTS, ETTUS Research, GSM, Software Defined Radio, Man-portable			<b>15. NUMBER OF PAGES</b> 119	
			<b>16. PRICE CODE</b>	
<b>17. SECURITY CLASSIFICATION OF REPORT</b> Unclassified	<b>18. SECURITY CLASSIFICATION OF THIS PAGE</b> Unclassified	<b>19. SECURITY CLASSIFICATION OF ABSTRACT</b> Unclassified	<b>20. LIMITATION OF ABSTRACT</b> UU	

THIS PAGE INTENTIONALLY LEFT BLANK

**Approved for public release; distribution is unlimited**

**GSM NETWORK EMPLOYMENT ON A MAN-PORTABLE UAS**

Darren J. Rogers  
Lieutenant, United States Navy  
B.S., Hawaii Pacific University, 2003

Submitted in partial fulfillment of the  
requirements for the degree of

**MASTER OF SCIENCE IN INFORMATION WARFARE SYSTEMS  
ENGINEERING**

from the

**NAVAL POSTGRADUATE SCHOOL  
September 2012**

Author: Darren J. Rogers

Approved by: Raymond R. Buettner, PhD  
Thesis Co-Advisor

Kevin D. Jones, PhD  
Thesis Co-Advisor

Dan C. Boger, PhD  
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

## **ABSTRACT**

There are numerous national systems that offer communications support with enhanced capabilities to support ISR. For the tactical unit, it can be challenging and cumbersome to deal with national systems that may or may not be able to provide near real-time support due to other, high priority tasking. The deployment of a low-cost GSM communications support system with enhanced capabilities (CSSEC) to support intelligence, surveillance and reconnaissance (ISR), which a tactical unit could have organically, would relieve the warfighter of having to depend on national assets and processes. Employing a CSSEC system on a man-portable or small UAS would allow the range of the system to be greatly extended, as opposed to a ground-based system which may be difficult to operate in a high-threat environment.

Commercial off-the-shelf (COTS) hardware is readily available and easily acquired. With a CSSEC deployed on a UAS, a tactical unit conducting ground operations would not be geographically constrained to a specific location to conduct ISR. Nor would they draw attention to the unit in having to set up antennas and other equipment on a building or outpost.

Leveraging COTS hardware and open-source software will keep overall cost low without having to deal with software licensing requirements associated with proprietary systems.

THIS PAGE INTENTIONALLY LEFT BLANK



# TABLE OF CONTENTS

<b>I.</b>	<b>INTRODUCTION.....</b>	<b>1</b>
<b>A.</b>	<b>PURPOSE.....</b>	<b>1</b>
<b>B.</b>	<b>BACKGROUND.....</b>	<b>1</b>
<b>C.</b>	<b>OBJECTIVE.....</b>	<b>2</b>
<b>D.</b>	<b>APPROACH.....</b>	<b>2</b>
<b>E.</b>	<b>ORGANIZATION.....</b>	<b>3</b>
<b>II.</b>	<b>UNMANNED AERIAL SYSTEMS.....</b>	<b>5</b>
<b>A.</b>	<b>HISTORY.....</b>	<b>5</b>
<b>B.</b>	<b>EXISTING DOD UAS.....</b>	<b>8</b>
1.	Classes and Categories.....	8
2.	Groups.....	11
<b>C.</b>	<b>CURRENT GROUP ONE UAS.....</b>	<b>13</b>
1.	Fixed Wing.....	13
a.	<i>Lockheed-Martin Stalker UAS.....</i>	<i>13</i>
b.	<i>Lockheed-Martin Desert Hawk III.....</i>	<i>15</i>
c.	<i>AeroVironment Puma AE (All Environment).....</i>	<i>16</i>
e.	<i>AeroVironment Raven.....</i>	<i>17</i>
f.	<i>AeroVironment Wasp AE.....</i>	<i>18</i>
g.	<i>Fixed Wing Summary.....</i>	<i>18</i>
2.	Vertical Take-off and Land (VTOL).....	19
a.	<i>AeroVironment Shrike/Qube.....</i>	<i>21</i>
b.	<i>Aeryon Scout.....</i>	<i>22</i>
c.	<i>Open Source VTOL.....</i>	<i>23</i>
d.	<i>Summary.....</i>	<i>25</i>
<b>III.</b>	<b>GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS (GSM).....</b>	<b>27</b>
<b>A.</b>	<b>HISTORY.....</b>	<b>27</b>
<b>B.</b>	<b>COVERAGE.....</b>	<b>27</b>
<b>C.</b>	<b>GSM NETWORK ARCHITECTURE.....</b>	<b>29</b>
1.	Mobile Station (MS).....	30
2.	Base Station Subsystem (BSS).....	31
a.	<i>BSC.....</i>	<i>31</i>
b.	<i>BTS.....</i>	<i>31</i>
3.	Network Subsystem.....	32
a.	<i>MSC.....</i>	<i>32</i>
b.	<i>HLR.....</i>	<i>33</i>
c.	<i>VLR.....</i>	<i>33</i>
4.	GSM Air Interface.....	33
a.	<i>Frequency Bands.....</i>	<i>33</i>
b.	<i>Absolute Radio Frequency Channel Numbers (ARFCN).....</i>	<i>34</i>
5.	GSM Frames and Call Setup.....	35
a.	<i>Control Channel Multiframe.....</i>	<i>37</i>

	<i>b.</i>	<i>Traffic Channel Multiframe</i> .....	38
	<i>c.</i>	<i>Initial Connection Process</i> .....	40
	<i>d.</i>	<i>Follow-On Connections</i> .....	41
IV.		<b>SOFTWARE-DEFINED RADIO (SDR)</b> .....	43
	A.	<b>INTRODUCTION</b> .....	43
	B.	<b>BACKGROUND</b> .....	43
	C.	<b>COMMERCIAL COMMUNICATIONS USE</b> .....	44
	D.	<b>MILITARY COMMUNICATIONS USE</b> .....	44
	E.	<b>SDR ARCHITECTURE</b> .....	45
		1. <b>ADC</b> .....	48
		2. <b>The Universal Software Radio Peripheral</b> .....	50
		3. <b>Software: GNU Radio</b> .....	53
	F.	<b>SUMMARY</b> .....	55
V.		<b>SMALL FORM FACTOR GSM SYSTEM</b> .....	57
	A.	<b>INTRODUCTION</b> .....	57
	B.	<b>HARDWARE</b> .....	57
		1. <b>USRP Ettus Research E100 SDR System</b> .....	57
		<i>a.</i> <i>COM Gumstix Overo</i> .....	59
		2. <b>Test Handsets</b> .....	60
	C.	<b>SOFTWARE</b> .....	61
		1. <b>Operating System: Ångström Linux</b> .....	61
		2. <b>SDR: GNU Radio</b> .....	62
		3. <b>OpenBTS</b> .....	63
		4. <b>SQLite</b> .....	64
		5. <b>Asterisk VoIP PBX</b> .....	64
		6. <b>System of Software</b> .....	66
	D.	<b>LAB BUILD AND TESTING</b> .....	67
		1. <b>Acquiring OpenBTS</b> .....	67
		2. <b>Build and Install</b> .....	67
		3. <b>Configuration</b> .....	67
		4. <b>Initial Run</b> .....	68
		5. <b>Testing Asterisk Configuration</b> .....	72
		6. <b>Testing SENDSMS Function</b> .....	74
		7. <b>Wi-Fi vs Ethernet Networking</b> .....	75
		8. <b>Size, Weight and Power</b> .....	76
		9. <b>Conclusions/Observations</b> .....	77
	E.	<b>INITIAL GROUND TESTING MONTEREY, CA MAY 18, 2012</b> .....	78
		1. <b>Conclusions/Observations</b> .....	80
	F.	<b>CAMP ROBERTS TNT 12-04 TESTING AUGUST 6, 2012</b> .....	80
		1. <b>Observations</b> .....	81
VI.		<b>CONCLUSIONS AND RECOMMENDATIONS</b> .....	83
	A.	<b>CONCLUSIONS</b> .....	83
		1. <b>Timing Accuracy</b> .....	83
		2. <b>RF Isolation</b> .....	83

3.	Flexibility .....	84
4.	Locked Handheld Devices .....	84
5.	Femtocells .....	85
6.	Fixed Wing vs VTOL.....	85
7.	Concept of Operations (CONOPS) .....	85
B.	RECOMMENDATIONS.....	86
1.	Technical.....	86
2.	Research.....	86
3.	Alternative CONOPS.....	86
4.	Adversary Use .....	86
LIST OF REFERENCES .....		87
INITIAL DISTRIBUTION LIST .....		93

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF FIGURES

Figure 1.	U.S. Navy assault drone (From Zaloga, 2008) .....	6
Figure 2.	AN/USD-1 (MQM-57 Falconer) (From Naughton, 2005) .....	7
Figure 3.	Airspace classification (From U.S. Department of Transportation Federal Aviation Administration, 2008) .....	10
Figure 4.	Lockheed-Martin Stalker UAS (From Lockheed-Martin, 2012) .....	14
Figure 5.	Lockheed-Martin Desert Hawk III UAS (From Lockheed-Martin, 2012) .....	15
Figure 6.	DHIII GCS and DHIII UAS (From Lockheed-Martin, 2012) .....	16
Figure 7.	AeroVironment common GCS (From U.S. Army, 2010) .....	17
Figure 8.	U.S. Army UAS near-term implementation (From U.S. Army, 2010) .....	20
Figure 9.	Microchip evolution 2005–2012 (From Anderson, 2012) .....	21
Figure 10.	AeroVironment Qube and Shrike VTOL (From AeroVironment, 2012) .....	22
Figure 11.	Aeryon Scout VTOL UAS (From Aeryon, 2012) .....	23
Figure 12.	3D Robotics' ArduCopter kit (From DIY Drones, 2012) .....	24
Figure 13.	ArduCopter Mission Planner GUI (From ArduCopter, 2012) .....	25
Figure 14.	GSM world frequency coverage (From Spareone, 2012) .....	28
Figure 15.	Mobile market share (From Global Mobile Suppliers Association, 2010) .....	29
Figure 16.	GSM architecture (From Stallings, 2005) .....	30
Figure 17.	Components of mobile station (From Noldus, 2006) .....	31
Figure 18.	IMSI composition (From Noldus, 2006) .....	31
Figure 19.	Base station subsystem: (a) wired, (b) wireless (From Bannister, Mather, & Coope, 2004) .....	32
Figure 20.	200-kHz GSM uplink channels (From Bannister, Mather, & Coope, 2004) .....	34
Figure 21.	GSM TDM frame structure (From Stallings, 2005) .....	36
Figure 22.	Timeslot in the downlink direction (From Sauter, 2011) .....	39
Figure 23.	Initial connection process (From Bannister, Mather, & Coope, 2004) .....	40
Figure 24.	SS7 network (From Bannister, Mather, & Coope, 2004) .....	42
Figure 25.	SPEAKeasy form factors (From Bonsor, 1998) .....	45
Figure 26.	Analog (a) and digital (b) hardware receivers (From Valerio, 2008) .....	46
Figure 27.	SDR-based radio implementation (From Eged & Babjak, 2006) .....	47
Figure 28.	SDR implementation levels (From Eged & Babjak, 2006) .....	47
Figure 29.	USRP simplified block diagram (From Valerio, 2008) .....	51
Figure 30.	GNU Radio GUI .....	54
Figure 31.	GNU Radio oscilloscope and FFT plots .....	55
Figure 32.	Traditional GSM network (top), notional OpenBTS network (bottom) (From Spicer, 2010) .....	57
Figure 33.	Ettus Research USRP E100 block diagram (From Ettus Research LLC, 2012) .....	58
Figure 34.	Gumstix Overo COM (From Gumstix, 2012) .....	59
Figure 35.	E100 with RFX900 installed .....	60
Figure 36.	Test handsets .....	61
Figure 37.	GNU Radio GUI showing GSM850 downlink .....	63

Figure 38.	Interaction of “sip.conf” and “extentions.conf” (From Madsen, Van Meggelen, & Bryant, 2011) .....	65
Figure 39.	Overview of software interaction (From Range Networks, 2012) .....	66
Figure 40.	OpenBTS build CLI (From Range Networks, 2012).....	67
Figure 41.	OpenBTS build CLI specific to ARM processor (From GNU Radio, 2011) ..	67
Figure 42.	OpenBTS.cpp TRX sleep value adjustment .....	68
Figure 43.	Five terminal windows running and monitoring the system.....	70
Figure 44.	OpenBTS CLI .....	71
Figure 45.	GSM900 test handsets registered to NPS network .....	72
Figure 46.	Testing the Asterisk dialplan .....	73
Figure 47.	Text message sent via OpenBTS CLI.....	74
Figure 48.	Text message received on handset.....	75
Figure 49.	Weight of E100 components.....	76
Figure 50.	Test network and E100 BTS .....	78
Figure 51.	E100 BTS mounted on vehicle .....	79
Figure 52.	Mast-mounted E100.....	81
Figure 53.	Test points A-J around McMillan Airfield .....	82

## LIST OF TABLES

Table 1.	Classes of Airspace (From Department of Defense, 2009) .....	9
Table 2.	Alignment of UAS (From Department of Defense, 2009) .....	11
Table 3.	Joint Unmanned Aerial System Concept of Operations UAS Categories (From Department of Defense, 2009) .....	11
Table 4.	Lockheed-Martin Stalker and Stalker XE Characteristics (From Lockheed- Martin, 2012) .....	14
Table 5.	Fixed wing parameter comparison.....	19
Table 6.	AFRCNS and associated radio channels (From Telecom ABC, 2005) .....	35
Table 7.	ADC Resolution 3-bit to 12-bit comparison .....	49
Table 8.	USRP parameters (From Ettus Research LLC, 2012) .....	52
Table 9.	Available daughterboards (From Ettus Research, LLC, 2012).....	52
Table 10.	List of GNU Radio modules (From Valerio, 2008).....	53
Table 11.	OpenBTS Initial Database Setup .....	68
Table 12.	Asterisk parameters.....	72
Table 13.	Test results at points A-J.....	82

THIS PAGE INTENTIONALLY LEFT BLANK



## **LIST OF ACRONYMS AND ABBREVIATIONS**

A	Amp
ADC	Analog-to-Digital
AE	All Environment
AEWE	Army Expeditionary Warrior Experiment
AGCH	Access Grant Channel
ANSI	American National Standards Institute
ARFCN	Absolute Radio Frequency Channel Number
ATC	Air Traffic Control
AuC	Authentication Center
BCCH	Broadcast Channel
BEC	Battery Elimination Circuit
BSC	Base Station Controller
BSS	Base Station Subsystem
BTS	Base Transceiver Station
CI	Cell Identifier
CLI	Command Line Interface
COM	Computer on Module
COTS	Commercial Off-the-Shelf
CPU	Central Processing Unit
DAC	Digital-to-Analog
DARPA	Defense Advanced Research Projects Agency
DC	Direct Current
DHIII	Desert Hawk III
DID	Direct Inward Dialing
DoD	Department of Defense
DSP	Digital Signal Processor
ELINT	Electronic Intelligence

EO	Electro Optical
FAA	Federal Aviation Administration
FACCH	Fast Associated Control Channel
FCCH	Frequency Correction Channel
FDMA	Frequency Division Multiple Access
FFT	Fast Fourier Transform
FL	Flight Level
FOSS	Free Open Source Software
FPGA	Field Programmable Gate Array
FPV	First Person View
FY	Fiscal Year
GCS	Ground Control Station
gMAV	Gasoline Micro Air Vehicle
GMT	Greenwich Mean Time
GNU	GNU is not Unix
GSA	Global Mobile Suppliers Association
GSM	Global System for Mobile Communications
GUI	Graphical User Interface
HLR	Home Location Register
HMMWV	High Mobility Multipurpose Wheeled Vehicle
IAI	Israeli Aircraft Industries
IF	Intermediate Frequency
IFR	Instrument Flight Rules
IMEI	International Mobile Equipment Identifier
IMSI	International Mobile Subscriber Identifier
IP	Internet Protocol
IR	Infra-red
ISR	Intelligence, Surveillance and Reconnaissance

ITU-T	International Telecommunications Union Telecommunications Standardization Sector
JTRS	Joint Tactical Radio System
kHz	Kilohertz
LAC	Location Area Code
LiPo	Lithium Polymer
LOS	Line-of-site
LRE	Launch and Recover Equipment
MCC	Mobile Country Code
MCE	Mission Control Element
ME	Mobile Equipment
MHHWV	High Mobility Multipurpose Wheeled Vehicle
MHz	Megahertz
MNC	Mobile Network Code
MS	Mobil Station
MSC	Mobile Switching Center
MSIN	Mobile Subscriber Identification Number
MSL	Mean Sea Level
NRT	Near Real Time
PBX	Private Branch Exchange
PCH	Paging Channel
PLMN	Public Land Mobile Network
PSTN	Public Switched Telephone Network
RACH	Random Access Channel
RAM	Random Access Memory
RC	Radio Controlled
RF	Radio Frequency
RX	Receive

S&A	See and Avoid
SACCH	Slow Associated Control Channel
SCH	Synchronization Control Channel
SCP	Service Control Points
SD	Secure Digital
SDCCH	Standalone Dedicated Control Channel
SDR	Software-Defined Radio
SIGINT	Signals Intelligence
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SMS	Short Message Service
SOI	Signal of Interest
SQL	Standard Query Language
SS7	Signaling System 7
SSP	Service Switching Points
STP	Signal Transfer Points
SUAS	Small Unmanned Aerial System
TCH	Traffic Channel
TCP	Transmission Control Protocol
TCXO	Temperature Compensated Crystal Oscillator
TDMA	Time Division Multiple Access
TRX	Transceiver
TX	Transmit
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicle
UCAV	Unmanned Air Combat Vehicle
UHD	USRP Hardware Driver
USAF	United States Air Force
USB	Universal Serial Bus

USRP	Universal Serial Radio Peripheral
VFR	Visual Flight Rules
VLR	Visitor Location Register
VoIP	Voice over IP
VTOL	Vertical Take Off and Land
WinSCP	Windows Secure Copy

THIS PAGE INTENTIONALLY LEFT BLANK

## **EXECUTIVE SUMMARY**

With nearly 4.5 billion subscribers worldwide, GSM is one of the most popular wireless communication technologies to date. Recent developments in open-source-software projects and software-defined radio technologies have enabled just about anyone to build a GSM network. While the focus of these developments has been to bring this wireless technology to economically depressed areas, it is worth looking at the possibility of these systems potentially supporting tactical intelligence, surveillance and reconnaissance (ISR) missions. National systems have enjoyed certain capabilities in this arena for some time; however, these systems are expensive, relatively low in number and in high demand, resulting in not being available for tactical unit operations.

Advances in microchip technology over the last five years has allowed small, backpackable unmanned aerial systems (SUAS) to become quite capable. By leveraging open source software and commercial off-the-shelf (COTS) hardware it is possible to build a low cost GSM system which can be deployed on a SUAS to enhance the ISR capabilities at the small, tactical unit level.

This thesis explores currently available COTS hardware and open source software to build a small-form factor GSM system capable of being deployed on a SUAS. A lightweight, small-form factor GSM system was built and tested with a range of just over 250 m. Enhancements in radio frequency isolation, amplification and computing capability, will increase the range to approach the GSM standard of 35 km.

THIS PAGE INTENTIONALLY LEFT BLANK



## **ACKNOWLEDGMENTS**

I would like to express my sincere gratitude to my thesis advisors, Dr. Raymond Buettner and Dr. Kevin Jones, for supporting me on this project. I have learned a lot during the course of my research and it has been a pleasure to work with both of them.

Thanks to Chuck Bokath and Allan Williams from the Georgia Tech Research Institute. Without their help and insight, I would not have been able to undertake this project.

Special thanks to Paul Buczynski for allowing me to use the EW lab for countless hours while I did initial system configuration.

Thanks to my Information Warfare Systems Engineering classmates of 2012, it has been quite a journey.

I would also like to express my thanks and dear appreciation to my wife, Lucy, who has taken care of so much while I spent many hours studying on campus. Without her support, my tour at NPS would have not been possible.

THIS PAGE INTENTIONALLY LEFT BLANK

# **I. INTRODUCTION**

## **A. PURPOSE**

Recent developments in technology and open source software have allowed the construction of intelligence, surveillance and reconnaissance (ISR) systems which were not previously available to the public. This thesis will explore currently available commercial off-the-shelf (COTS) hardware and open source software to assemble a small form factor GSM system capable of being integrated with currently available small unmanned aerial systems (SUAS).

## **B. BACKGROUND**

In the middle of 2007, a project called OpenBTS was started by three developers (Bort, 2010). Their goal was to develop software that would interact with a software-defined radio (SDR) and create, essentially, a GSM base transceiver station (BTS). OpenBTS would then use voice-over-IP (VoIP) to connect calls to the rest of the world.

By the middle of 2008, they had achieved their objective and were able to test their network on a large scale event in a desert in Nevada, called Burning Man. Shortly after their testing, the OpenBTS software was released as open source to the public. The idea for OpenBTS was to help bring GSM cellular coverage where it was not available or to countries who could not afford traditional infrastructure. This could also prove to be beneficial in places like Afghanistan where the Taliban has GSM network providers turn off BTSs in the evening or as they direct. This tactic is used by the Taliban to project their presence and show that they still have influence in the region. The Taliban has also employed this tactic to “degrade the enemy’s capability in tracking down our mujahedeen.” These tactics make daily cell phone reception a constant struggle (Rubin, 2011).

With the open source software and COTS hardware it has been possible for other people to experiment with building their own BTS for experimentation and research. Some of this research has included looking at vulnerabilities in cellular networks.

One example was demonstrated in January 2011 at the Washington, DC, Black Hat conference. A participant, using a laptop and OpenBTS, was able to send a message to a number of conference attendee's cell phones asking them to join a rogue GSM network (Messmer, 2011).

Another example of OpenBTS used in GSM cellular security research was provided at the BlackHat USA and DEFCON 19 conferences in the summer of 2011. Two researchers, Mike Tasse and Richard Perkins, gave a presentation which discussed their build of what they called a Wireless Aerial Surveillance Platform, which was built on a FMQ-117B U.S. Army surplus target drone airframe. Their payload consisted of, among other things, an Ettus Research universal software radio peripheral (USRP) and a computing device running OpenBTS. The payload would pose as a GSM cell network and would deceive cell phones to connect through their network (Dillow, 2011).

Taking this model and using it in an environment such as Afghanistan would enable coalition forces to overcome the problem of the Taliban shutting down GSM networks. Using a SUAS, a tactical unit would draw upon organic resources to provide GSM network service in an area where it has been suppressed by the Taliban. Coalition forces could also use the network as a way to push information via SMS keeping the local populace informed.

### **C. OBJECTIVE**

While the DoD has enjoyed certain capabilities in this, they come at a cost that often limits the utility to the ground soldier. This thesis will focus on building a small form factor GSM system capable of being integrated into a backpackable SUAS, by using COTS on open source software, which will cost substantially less than currently available systems.

### **D. APPROACH**

First, current SUAS will be evaluated for payload capacity which will allow for research and evaluation of available COTS hardware for viable payload solution. OpenBTS will be used to build and analyze a small form factor GSM system capability. The GSM system's effective range will be tested using test handsets. The COTS

hardware will be evaluated for size, weight and power considerations. Two main SUAS categories, vertical takeoff land (VTOL) and fixed wing, will be evaluated and compared.

## **E. ORGANIZATION**

A brief history of unmanned aerial systems (UAS), DoD categorization, and overview of currently available SUAS will be discussed in Chapter II. GSM history, air interface, logical channels and subsystems which make up a GSM network will be discussed in Chapter III. Software-defined radio (SDR) history, elementary concepts, SDR software and USRP hardware will be discussed in Chapter IV.

The small form factor GSM system build, configuration and testing will be discussed in Chapter V. It will include hardware and software requirements. Lab and field test results are also included.

Conclusions and recommendations for future research will be discussed in Chapter VI with an emphasis on whether or not the system can be feasibly used as previously discussed.

THIS PAGE INTENTIONALLY LEFT BLANK

## **II. UNMANNED AERIAL SYSTEMS**

Since 1991 Unmanned Aerial Systems (UAS) have seen an unprecedented growth in the U.S. Military. While UAS had been around and used for many years prior to the 1990s; advances in technology enabled them to deliver the support required for military combat operations starting with Operation Desert Storm in 1991. Since then UAS have permeated many more mission sets such as force protection, mine surveillance and even being lethal themselves. This chapter will discuss the history of UAS and current man-portable UAS options which could serve as a platform for a small form factor GSM system.

### **A. HISTORY**

UAS have been used by the military for nearly 100 years. The first examples of the use of UAS (referred to as remotely piloted aircraft at that point), took place in 1917 during World War I. Initial efforts were impeded by the technology available at the time. Most of the developments were focused on creating what would be described as a crude cruise missile by today's standards. Between WWI and WWII primitive UAS were largely used as targets to train anti-aircraft gunners. By 1941 technologies in flight control and radar guidance systems were mature enough for the military to sponsor a program where a UAS would deliver a weapon and return to base. This resulted in the Navy's first assault drone, the TDN-1 (Figure 1). The TDN-1 was used in the Pacific during 1944. It initially was used as a guided missile by targeting Japanese bunkers and gun positions. It was also used as an unmanned air combat vehicle (UCAV) where it would deliver a weapon and return to base. Having the TDN-1 safely return to base proved to be challenging. Similar concepts were attempted during the Korean War (Zaloga, 2008).

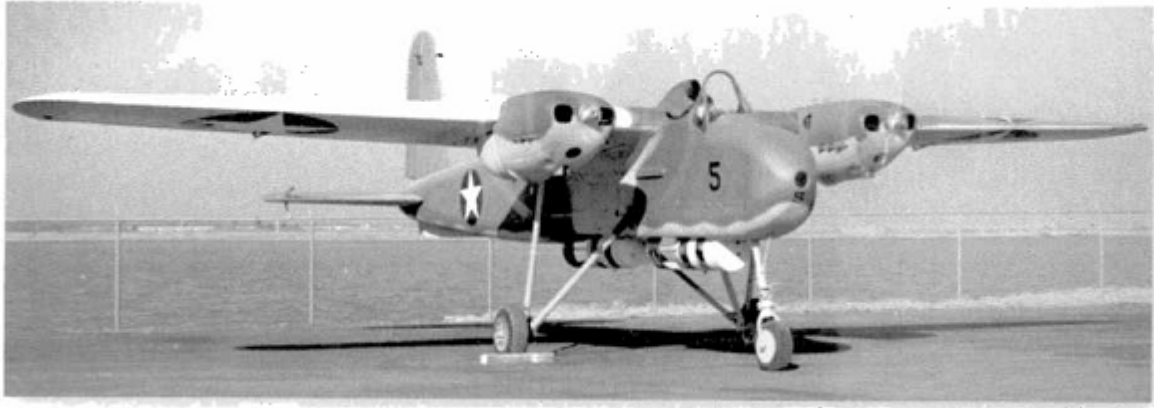


Figure 1. U.S. Navy assault drone (From Zaloga, 2008)

In the 1950s, the military started to explore outfitting UAS with camera equipment to be used for battlefield surveillance. The first successful surveillance UAS was the Army's AN/USD-1. The AN/USD-1 (renamed MQM-57 Falconer) is credited with pioneering most of the essential technologies used in UAS to this date (Figure 2). Many more programs followed the AN/USD-1 in the areas of surveillance. Research in weaponizing UAS had largely split off into the area of cruise missile development at this point. Surveillance UAS technologies had setbacks as well, in particular, the processing of intelligence was cumbersome. UAS would conduct reconnaissance; however, by the time it returned to base, had its camera film unloaded, developed and the photos analyzed, the information was anything but near real-time (NRT) (Zaloga, 2008). Developments in the late 1950s increased airborne reconnaissance capabilities in manned aircraft however, still requiring personnel on the air platform still had drawbacks.





Figure 2. AN/USD-1 (MQM-57 Falconer) (From Naughton, 2005)

The loss of two U-2 aircraft in the early 1960s increased the urgency to incorporate additional reconnaissance capabilities into UAS. The USAF developed the Ryan 147, also known as the Firebee, which had an electronics intelligence (ELINT) payload for detecting surface-to-air (SAM) missile threats. The Ryan 147 saw major use in the Vietnam War. The benefits of using UAS in missions deemed too dangerous for manned aircraft became apparent to military leadership during the Vietnam War. General John C. Meyer, Commander in Chief Strategic Air Command in 1973 pointed out, “We let the drone do the high-risk flying ... the loss rate is high, but we are willing to risk more of them ... they save lives!”

Developments in technologies between the Vietnam War and Operation Desert Storm allowed for significant improvements in control of UAS and real-time video downlink. The Pioneer UAS was developed in the late 1980s in partnership with Israeli Aircraft Industries (IAI). The Pioneer was capable of being launched and controlled from a battleship. This capability was used for battleship artillery adjustment during Operation

Desert Storm. The results were impressive, so much that an Iraqi military unit surrendered to a U.S. UAS knowing that their position would soon be receiving artillery (Zaloga, 2008).

## **B. EXISTING DOD UAS**

As of June 2011, the Department of Defense (DoD) has more than 6,000 unmanned aircraft (Congressional Budget Office, 2011). The DoD UAS range from large systems such as the Global Hawk down to small unit-level systems such as AeroVironment's Wasp UAS. The required infrastructure scales proportionally along with the aircraft it supports. Ground control systems (GCS) can be elaborate and occupy a building, scaled down to occupy a trailer or High Mobility Multipurpose Wheeled Vehicle (HMMWV) or small enough to be handheld. The DoD has shown the strategic importance of the UAS in current and future military operations through the development of dedicated UAS roadmaps such as the annually published, "DoD's Unmanned Systems Integrated Roadmap," which takes a look at integrating various unmanned systems over the next 25 years.

### **1. Classes and Categories**

With so many existing systems available, classifying different types of UAS becomes difficult. While some systems can be categorized based on size alone, the different branches of the military use a tiered classification system based on DoD guidance, the FAA uses an airspace classification system, and the DoD uses categories and groups based on FAA regulations (Table 1).

Table 1. Classes of Airspace (From Department of Defense, 2009)

Airspace Class	Description
A	Airspace exists from Flight Level (FL) 180 (18,000 feet mean sea level (MSL)) to FL600 (60,000 feet MSL). Flights within Class A airspace must be under instrument flight rules (IFR) and under the control of air traffic control (ATC) at all times.
B	Airspace generally surrounds major airports (generally up to 10,000 feet MSL) to reduce mid-air collision potential by requiring ATC control of IFR and Visual Flight Rules (VFR) flights in that airspace.
C	Airspace surrounds busy airports (generally up to 4000 feet AGL) that do not need Class B airspace protection and requires flights to establish and maintain two-way communications with ATC while in that airspace. ATC provides radar separation service to flights in Class C airspace.
D	Airspace surrounds airports (generally up to 2500 feet AGL) that have an operating control tower. Flights in Class D airspace must establish and maintain communications with ATC, but VFR flights do not receive separation service.
E	Airspace is all other airspace in which IFR and visual flight rules (VFR) flights are allowed. Although Class E airspace can extend to the surface, it generally begins at 1200 feet AGL, or 14,500 feet MSL, and extends upward until it meets a higher class of airspace (A–D). It is also above FL600.
G	Airspace (there is no Class F airspace in the United States) is also called “uncontrolled airspace” because ATC does not control aircraft there. (ATC will provide advisories upon request, workload dependent.) Class G airspace can extend to 14,499 feet MSL, but generally exists below 1200 feet AGL and below Class E airspace.
Note: Classes B, C, and D relate to airspace surrounding airports (terminal airspace) where increased mid-air collision potential exists; Classes A, E, and G primarily relate to altitude and the nature of flight operations that commonly occur at those altitudes (en route airspace).	

A graphical representation of the airspace classes listed in Table 1 is shown in Figure 3. Class B, C and D are specific to airspace in the vicinity of airports.

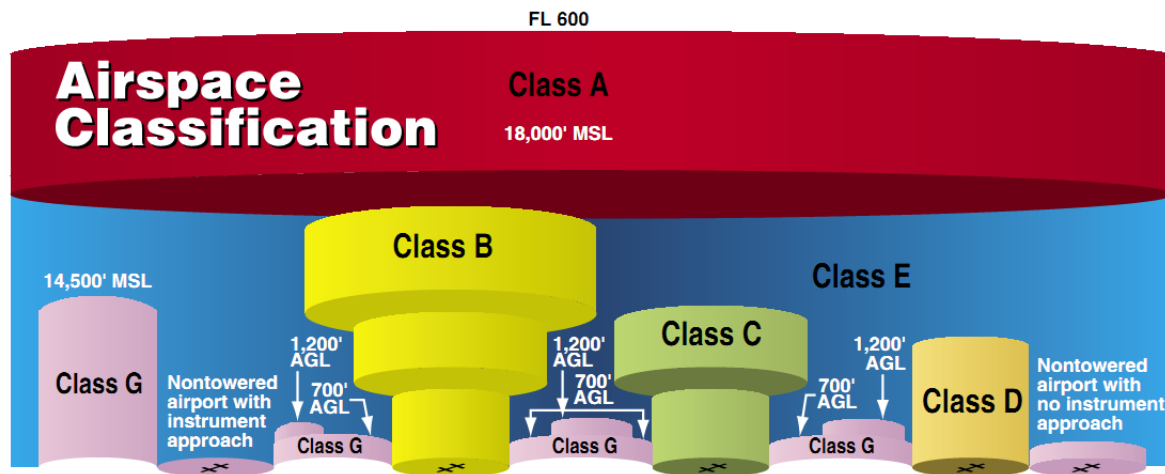


Figure 3. Airspace classification (From U.S. Department of Transportation Federal Aviation Administration, 2008)

The DoD then categorizes UAS based on FAA airspace classes in the following manner:

- UAS (Cat III). Capable of flying throughout all categories of airspace and conforms to Part 91 (i.e., all the things a regulated manned aircraft must do including the ability to see and avoid (S&A)). Airworthiness certification and operator qualification are required. UAS are generally built for beyond line-of-sight (LOS) operations. Examples: Global Hawk, Predator (Department of Defense, 2009).
- UAS (Cat II). Nonstandard aircraft that perform special purpose operations. Operators must provide evidence of airworthiness and operator qualification. Cat II UAS may perform routine operations within a specific set of restrictions. Example: Shadow (Department of Defense, 2009).
- UAS (Cat I). Analogous to RC models as covered in [FAA's Model Aircraft Operating Standards]. Operators must provide evidence of airworthiness and operator qualification. Small UAS are generally limited to [first person view (FPV)] operations. Examples: Raven, Dragon Eye (Department of Defense, 2009).

Examples of UAS categories I through III, how they line up with airspace usage and FAA regulations is shown in Table 2

Table 2. Alignment of UAS (From Department of Defense, 2009)

		<b>Certified Aircraft / UAS (CAT III)</b>	<b>Nonstandard Aircraft / UAS (CAT II)</b>	<b>RC Model Aircraft / UAS (CAT I)</b>
FAA Regulation		14 CFR 91	14 CFR 91, 101, and 103	None (AC 91–57)
Airspace Usage		All	Class E, G, & non-joint-use Class D	Glass G (<1200 ft AGL)
Airspeed Limit, KIAS		None	NTE 250 (proposed)	100 (proposed)
Example Types	Manned	Airliners	Light-Sport	None
	Unmanned	Predator, Global Hawk	Shadow	Dragon Eye, Raven

## 2. Groups

The DoD further divides the categories into groups based on gross takeoff weight, operating altitude and airspeed (Table 3).

Table 3. Joint Unmanned Aerial System Concept of Operations UAS Categories (From Department of Defense, 2009)

UAS Category	Maximum Gross Takeoff Weight (lbs)	Normal Operating Altitude (ft)	Speed (Knots Indicated Airspeed)	Example UAS
Group 1	0–20	<1,200 AGL	100 kts	WASP III, RQ-16A, Pointer, Aqua/Terra Puma
Group 2	21–55	<3,500 AGL	<250 kts	ScanEagle
Group 3	<1,320	<18,000 AGL		RQ-7B, RQ-15, STUAS
Group 4	>1320		Any Airspeed	MQ-5B, MQ-8B, MQ-1A/B/C, A-160
Group 5				>18,000 AGL

Groups two through five are considered to be non-man-portable due to not only their weight alone but also the ground control station requirements. While the weight listed for group two would make it seem that they are man-portable, the vehicles usually require an additional launching mechanism. The physical dimensions of the group two UAS can make the system unwieldy to carry. Groups two through three are often referred to as medium-sized UAS, while groups four and five are referred to large-sized UAS (Congressional Budget Office, 2011).

Group five UAS enjoys long endurance and large payload capacity. The Global Hawk has an endurance of 32 hrs and a payload capacity of up to 3,000 lbs (Department of Defense, 2009). It needs a developed runway for takeoff and landing. It supports the warfighter at the theater level and has an abundance of sensors for intelligence, surveillance and reconnaissance (ISR). It requires a Launch and Recover Element (LRE) and a Mission Control Element (MCE) to operate. Three crewmembers are required to fly Global Hawk: LRE Pilot, MCE Pilot and Sensor Operator (USAF, 2012). The Congressional Budget Office lists the cost of the Global Hawk program at \$1.2 billion in 2011 (Congressional Budget Office, 2011). The U.S. Air Force currently has 20 in its inventory. The limited number of Global Hawks throughout the DoD makes the tasking of the resource strictly controlled at the theater level. In order for a tactical unit to take advantage of a Global Hawk asset, tasking must be fully vetted up the chain of command to the theater commander, which can be time consuming and cumbersome.

Other UAS that fall into either group 4 or 5 are the MQ-1 Predator, MQ-9 Reaper, MQ-5 Hunter and the MQ-1C Grey Eagle. The MQ designation for these platforms indicates that they are not only for reconnaissance, but have a multi-mission capability which includes carrying a lethal payload. The RQ-7 Shadow is used only for reconnaissance and does not have the ability to carry a lethal payload, hence the RQ designator.

While groups two through five offer large flexible payloads, group one is enjoying recent advances in technology thus reducing the form factor of both avionics and general electronic payloads. Group one and sometimes group two UAS are not programs of record which reduces the timeline from concept to deployment.

Technologies that were once employed only in the larger UAS can now be deployed in man-portable UAS. Endurance is still not very long since power is still an issue as more electronics are packed into the form factor, the need for more electrical power increases however; even this area has seen some improvements with enhancements in battery technology and alternative fuel sources.

The next section will look at current DoD group one platforms in use, some alternative platforms available and then look at COTS open source platforms that are currently accessible on the commercial market. As the cost of technology continues to drop, group one UASs will continue to benefit with enhanced capabilities.

### **C. CURRENT GROUP ONE UAS**

In order to take a look at the current man-portable (group one) UASs available, we will look at two categories: fixed wing and vertical take-off and landing (VTOL)

#### **1. Fixed Wing**

Current fixed wing man-portable UAS are being developed by a wide number of DoD contractors. Rather than look at all current models being developed, we will focus Lockheed-Martin and AeroVironment, who have demonstrated their platforms in the man-portable UAS category and have their products in the current DoD inventory.

##### ***a. Lockheed-Martin Stalker UAS***

Lockheed-Martin offers two different variants of their Stalker UAS: Stalker and Stalker eXtended Endurance (Stalker XE) (Figure 4). The Stalker can be hand launched or launched by a bungee cord ground launching system. The Stalker XE can only be launched by the bungee cord system. Both variants are recovered using a, not too gracious, deep stall method, which eliminates the need for a runway and minimizes the concern for wind direction during recovery. The Stalker and Stalker XE can be operated by one or two operators from a laptop-based ground control station (GCS). The primary payload is an image sensor capable of high-definition images during day and night. Both variants are outfitted with a compartment that allows the UAS to drop a payload from the air. The Stalker is powered by Lockheed-Martin's Hush Drive electric system which

allows for a maximum flight time of over two hours, payload weight capability of three pounds and makes the Stalker UAS inaudible above 400 ft. The Stalker XE is powered by a solid oxide fuel cell which increases the flight time to over eight hours. What the Stalker XE makes up for in flight time it loses in payload weight capability by decreasing it to two pounds. The XE's wingspan is also increased to 12 feet. (Lockheed-Martin, 2012). While it is considered man-portable, the 10 and 12 foot wingspans make them unwieldy to haul around without a vehicle. A comparison of the Stalker and Stalker XE parameters is shown in Table 4.



Figure 4. Lockheed-Martin Stalker UAS (From Lockheed-Martin, 2012)

Table 4. Lockheed-Martin Stalker and Stalker XE Characteristics (From Lockheed-Martin, 2012)

<b>Parameter</b>	<b>Stalker</b>	<b>Stalker XE</b>
Payload	3 lbs	2 lbs
Flight Time	2+ hours	8+ hours
Altitude	15,000 ft	15,000 ft
Speed	50 mph dash	45 mph dash
Propulsion	Electric	Solid Oxide Fuel Cell
Launch	Hand or bungee	Bungee
Max Take-off Weight	17.5 lbs	22 lbs
Wingspan	10 feet	12 feet



***b. Lockheed-Martin Desert Hawk III***

Another of one of Lockheed-Martin's fixed wing UAS, Desert Hawk III (DHIII) was demonstrated at the annual Army Expeditionary Warrior Experiment (AEWE) in 2011 (Figure 5). The DHIII is smaller and more lightweight than the Stalker UAS. It weighs 8.2 lbs (with payload) and has a wingspan of 4 ft 11 inches. The UAS and the GCS are backpackable but each system requires a separate backpack for a total of two. The UAS backpack has a total weight of 36 lbs and the GCS weighs 15 lbs (Figure 6). The DHIII must be assembled prior to flight. The assembly takes 10 minutes, which may or not be feasible depending on the tactical environment. The DHIII is hand-launched and recovered via a skid landing. It has a modular payload capability allowing for flexibility for different tactical situational requirements. Up to four DHIIIs can be controlled from one GCS. The GCS is laptop-based which does not readily support hand-held operation since the operator will need to put the laptop on a table or the ground. The DHIII has an autopilot function which allows an operator to focus on the mission set and not necessarily flying the UAS (Lockheed-Martin, 2012). DHIII has a low audio signature, has been used by British Army forces and was well received by the U.S. Army at AEWE (Bacon, 2011).



Figure 5. Lockheed-Martin Desert Hawk III UAS (From Lockheed-Martin, 2012)



Figure 6. DHIII GCS and DHIII UAS (From Lockheed-Martin, 2012)

*c. AeroVironment Puma AE (All Environment)*

AeroVironment's Puma fixed wing UAS is slightly smaller than Lockheed-Martin's Stalker with a wingspan of 9.2 ft. It weighs 13 lbs, which allows it to be hand launched as well. Similar payloads are available to support ISR day or night. Its maximum altitude is 10,000 ft which is slightly less than the Stalker UAS. It is battery powered which makes it quiet and enables a flight time of two hours. It can be operated by one operator or two. With one operator, the Puma can be programmed to fly GPS way points allowing the operator to focus on the mission set. The GCS is handheld and can be used to control other AeroVironment UASs such as the Raven and Wasp (Figure 7). Having the GCS in a hand-held form factor greatly reduces the required equipment to enable use of the Puma. Puma has a payload capacity of 4 lbs and a range of 15 km (AeroVironment, 2012). Puma is hand-launched and recovered using a deep stall method. It is the largest of the AeroVironment man-portable UAS, but like the Stalker UAS, its 9ft wingspan makes it difficult to transport without a vehicle.



Figure 7. AeroVironment common GCS (From U.S. Army, 2010)

*e. AeroVironment Raven*

With a wingspan of 4.5 ft, AeroVironment's Raven UAS is about half the size of the Puma UAS. It is battery powered, hand-launched and has a line-of-site range of 10km. With its small wingspan, weight of 4.2 lbs and hand-held GCS, it is truly man-portable. It has an endurance of up to 90 minutes. It is limited to a payload capacity of 6.5 oz (184g). Its primary payload is composed of electro-optical (EO) and infra-red (IR) cameras. The U.S. Army has found great success in utilizing the Raven in combat operations.

MOS non-specific personnel can program, launch, fly, retrieve, and maintain the Raven. Fielding for the [Raven] has been underway since June 2006 to both active and reserve components brigade combat teams (BCT) and armored cavalry regiments. The Raven is the Joint [small UAS] of choice currently supporting operations in OIF and OEF. (U.S. Army, 2010)

*f. AeroVironment Wasp AE*

AeroVironment's Wasp AE has a wingspan of just 3.3 ft and is their smallest UAS next to the Wasp III. It is a slightly modified version of the Wasp III, which was developed in a joint effort between AeroVironment and the Defense Advanced Research Projects Agency (DARPA). It has integrated high-resolution EO and IR payloads. While the Wasp III weighs just 1lb, the more robust Wasp AE weighs 2.85 lbs. The Wasp AE is hand-launched, backpackable and has a flight time of 50 minutes. With its battery powered motor and small form factor it can go virtually undetected (AeroVironment, 2012). The Wasp AE, like other fixed wing UAS, is recovered using a deep stall method. As of May 2012, the USAF budgeted \$2.5 million to include the Wasp AE in their Battlefield Air Targeting Micro Air Vehicle (BATMAV) program (Warwick, 2012).

*g. Fixed Wing Summary*

Fixed wing UAS offer a lot of options for giving ground forces an "eye in the sky." Most fixed wing group one and two UAS require to be hand-launched thus opening the possibility for personnel on the ground to expose themselves to the enemy. Fixed wing man-portable UAS are not inexpensive. In 2006, the USAF listed AerovVironment's Wasp III as \$49,000.00 (US Airforce, 2011) and there were 200 in inventory according to the 2009 Unmanned Systems Integrated Roadmap (Department of Defense, 2009). Fixed wing UAS are not as maneuverable as vertical take-off and land (VTOL), but can offer higher endurance flight times and the smaller form factors can have limited payload capabilities. Table 5 shows a comparison of key fixed wing parameters.

Table 5. Fixed wing parameter comparison

<b>UAS</b>	<b>Wingspan</b>	<b>Endurance</b>	<b>Launch Mechanism</b>	<b>Power</b>	<b>Payload Capacity</b>
Stalker	10'	2+ hrs	Hand or bungee	Electric	3 lbs
Stalker XE	12'	8+ hrs	Bungee	Solid Oxide Fuel Cell	2 lbs
Desert Hawk III	4'11"	90 mins	Hand	Electric	2 lbs
AV Puma	9.2'	2 hrs	Hand	Electric	4 lbs
AV Raven	4.5'	90 mins	Hand	Electric	6.5 oz
AV Wasp	3.3'	50 mins	Hand	Electric	275 grams

## 2. Vertical Take-off and Land (VTOL)

VTOL UAS have been gaining in popularity due to their hover, perch and stare capabilities. Another benefit is that VTOL UAS need very little, if any, launch equipment which is beneficial in constrained environments and for keeping soldiers undercover. In the U.S. Army Roadmap for SUAS 2010–2035 VTOL is listed as being integrated in FY2013 and being labeled “niche capability” (Figure 8). Small, man-portable VTOL are largely missing from DoD and Army Unmanned Systems Roadmaps. Mid-term Army UAS Development Considerations: Raven fully deploy, VTOL UAS reach full operational capability. Far-term Army UAS Development Considerations: “The VTOL technologies will close the performance and airworthiness gaps with fixed wing systems, including rotor, propulsion, airframe and hybrid configurations providing point-to-point capability” (U.S. Army, 2010). The Gasoline Micro Air Vehicle (gMAV) is the one man-portable VTOL that is listed in the DoD UAS Roadmap.

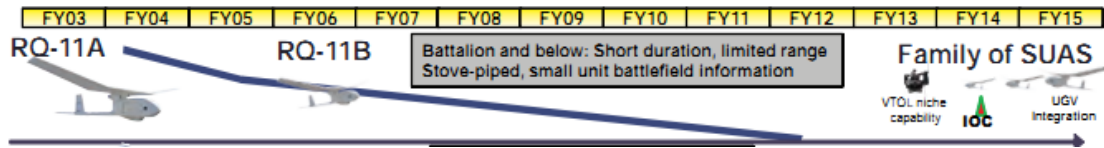


Figure 8. U.S. Army UAS near-term implementation (From U.S. Army, 2010)

The gMAV is manufactured by Honeywell and is powered by a two stroke gas engine. The gMAV's gas powered engine makes it quite loud, so it is most suited for missions where stealth is not required. Some examples would include land mine surveillance and battle damage assessment missions.

It appears that most of 2009–2011 has seen, above all, research and development (R&D) in man-portable VTOL UAS and little acquisition aside from the gMAV. There has been a significant amount of research occurring in both military and civilian domains. While the military typically enjoys cutting edge technology before civilians have access to it, the gap is shrinking. A recent article in Wired magazine showcased the fact that, "Today's personal [UAS] have benefited from the same advances in technology that have made the iPhone so powerful" (Anderson, 2012). Since 2005, microchip technology has allowed the capability of what once required six different chips to be bundled up into one (Figure 9).



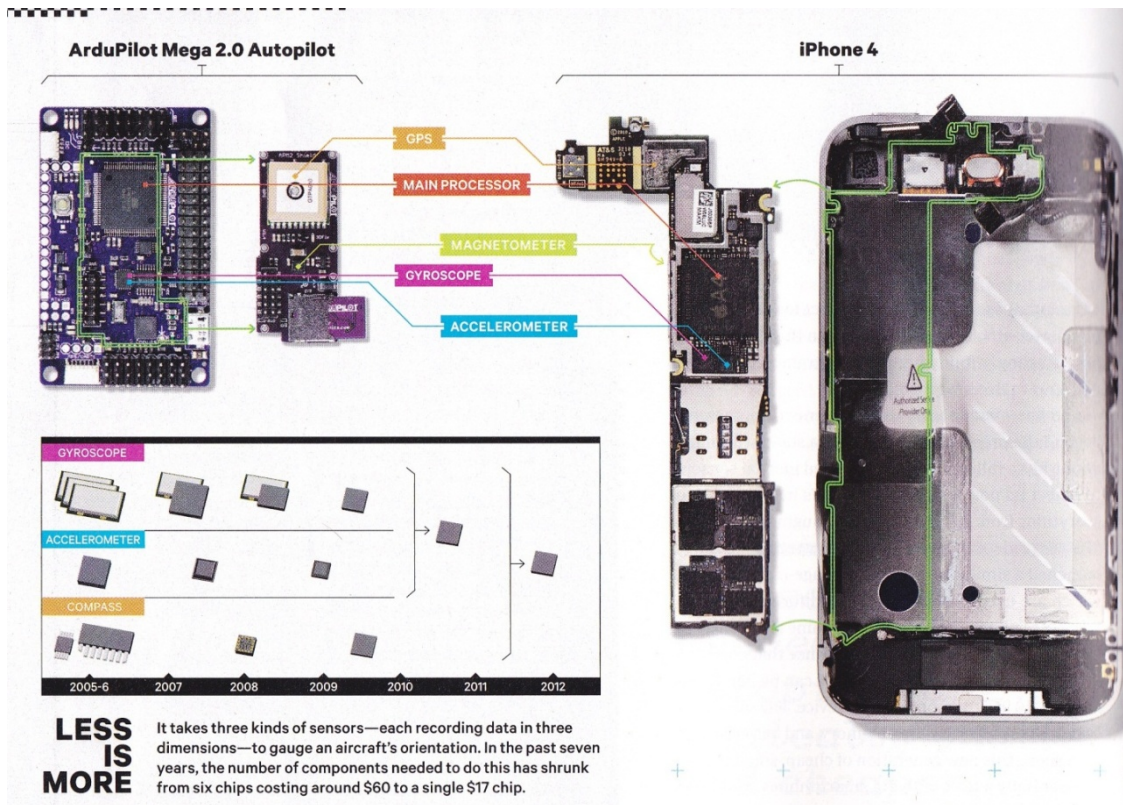


Figure 9. Microchip evolution 2005–2012 (From Anderson, 2012)

As of July 2012, Lockheed-Martin did not have a backpackable VTOL listed in their portfolio, however they acquired a company called Procerus Technologies earlier in the year (Lockheed-Martin, 2012). This acquisition may indicate that Lockheed-Martin may be developing a backpackable VTOL in the near future. AeroVironment has developed two quadrotor variants one is marketed as a “public safety small UAS” and is called Qube. The other is listed under “advanced development” and named Shrike.

*a. AeroVironment Shrike/Qube*

The Qube and Shrike quadrotors appear to be built on the same airframe, but are targeted to different mission sets (Figure 10). The Qube is targeted for law enforcement and public safety. Shrike is targeted for covert military mission sets and was a project developed out of a DARPA contract. Both variants are listed as having a flying time of 40 minutes and a weight of 5.5 lbs. The ranges however, are significantly different. Where the Qube’s range is 1km line-of-sight (LOS), the Shrike’s range is 5km

LOS. Both carry high resolution EO and IR cameras. One of the benefits of the VTOL is that while it has a 40 minute flight time, it can transmit video for several hours when it is operated in sit and stare mode. The Shrike will operate with AeroVironment's existing GCS that is used for Puma, Raven and Wasp (Business Wire, 2011).



Figure 10. AeroVironment Qube and Shrike VTOL (From AeroVironment , 2012)

***b. Aeryon Scout***

A Canadian company by the name of Aeryon has developed a small quadrotor VTOL UAS called Scout (Figure 11). Aeryon has showcased the Scout being used by Libyan rebels for reconnaissance missions as well as by BP in Alaska for potential oil spill response efforts (Aeryon, 2011). Its flight time is relatively short at 25 minutes when compared to AeroVironment's VTOL UAS models. It can carry a payload weight of up to 400 grams and has a range of up to 3 km. Its range does not have to be LOS as it will fly pre-programmed GPS way points and has a fail-safe return to home function. It is outfitted with high resolution EO and IR cameras. The entire system is backpackable and can be setup in seconds.





Figure 11. Aeryon Scout VTOL UAS (From Aeryon , 2012)

### *c. Open Source VTOL*

The systems previously discussed have all been proprietary in nature. They are designed, built and configured by companies who will demand market pricing. With inexpensive sensors, COTS hardware and open-source software nearly anyone can build a VTOL UAS at an affordable price (Anderson, 2012). ArduCopter is one example of an affordable “complete [UAS] solution, offering both remote control and autonomous flight, including waypoints, mission planning and telemetry displayed on a powerful ground station” (ArduCopter, 2012). ArduCopter is the actual name of the “Arduino-based autopilot for multicopter craft” (ArduCopter, 2012) and not necessarily the airframe. Fully assembled or disassembled kits are available from assorted vendors such as 3D Robotics based in San Diego, CA (Figure 12) and a base kit retails for under \$600.00.



Figure 12. 3D Robotics' ArduCopter kit (From DIY Drones, 2012)

Due to the various different configurations available such as motor type, battery type, propeller size, etc it is hard to determine standard payload capacity, range and flight time (10–20mins). The airframe is just over two feet at its widest point (25.45”) which makes it slightly smaller than the Aeryon Scout (31.5”). An example of average flight time is nine minutes with a 300 g payload (jDrones).

The ArduCopter is controlled by a GCS usually comprised of a laptop running the free software Mission Planner or a digital radio control set. Mission Planner allows for GPS waypoint entry, loitering function, return to home, automatic takeoff and landing, auto-level and altitude control. These features are all commonly found in more sophisticated UAS designs.



Figure 13. ArduCopter Mission Planner GUI (From ArduCopter, 2012)

#### d. Summary

UAS has come a long way since the concept was first explored in WWI. Recent developments in technology have allowed group one UAS to increase in utility immensely. VTOL R&D will continue to add more capability in smaller airframes. Improved battery and fuel technologies will increase flight times. Future DoD and service UAS roadmaps will start to include a variety of man-portable VTOL UAS as formal acquisitions begin. Civilian entities will continue to have access to more robust UAS technologies which may lead to problems if UAS are employed for unacceptable uses.

THIS PAGE INTENTIONALLY LEFT BLANK

### **III. GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS (GSM)**

This chapter gives an overview of the GSM system in order to understand the different components and systems which make it up. This will help determine the design requirements for building a GSM system, as discussed in Chapter V.

#### **A. HISTORY**

In Europe a group was formed to investigate a standard mobile system for use in the various countries across the continent. The group was appointed by the European Conference of Postal and Telecommunications Administrations and was known as Groupe Special Mobile. This is initially where the acronym, GSM, came from. GSM is commonly referred to today as global system for mobile communications. GSM was introduced in Europe 1990. North America was late to adopt the GSM standard because it did not have to deal with multiple mobile standards across its geographic region (Bannister, Mather, & Coope, 2004). North America started using Advanced Mobile Phone Service (AMPS) in the early 1980s. IS-136 (D-AMPS) replaced AMPS and the wireless network providers eventually moved to the GSM standard. AMPS was entirely replaced by 2008, when network providers decommissioned it (Lawson, 2008).

#### **B. COVERAGE**

While there are other technologies and standards available, GSM has grown to cover the majority of the global mobile market share to date. A company by the name of SpareOne, markets a GSM phone which is powered by single AA battery to be used in case of emergencies. SpareOne shows the global GSM coverage with a map on their website which makes it clear that GSM coverage is worldwide (Figure 14). Of the major nation states, Japan and South Korea are not covered by GSM.



Figure 14. GSM world frequency coverage (From Spareone, 2012)

Along with worldwide coverage GSM has impressive numbers for mobile subscribers. The Global Mobile Subscribers Association (GSA) has recent numbers showing that the numbers are approaching 4.5 billion of GSM mobile subscribers (Figure 15), making GSM the most widely adopted wireless technology in the world. Its popularity has driven primarily by allowing mobile subscribers to travel to different countries and still be able to use their mobile device. Proprietary technologies, such as code division multiple access (CDMA) used by Verizon Wireless, require subscribers to change their mobile device in order to be able to use wireless networks in different countries.

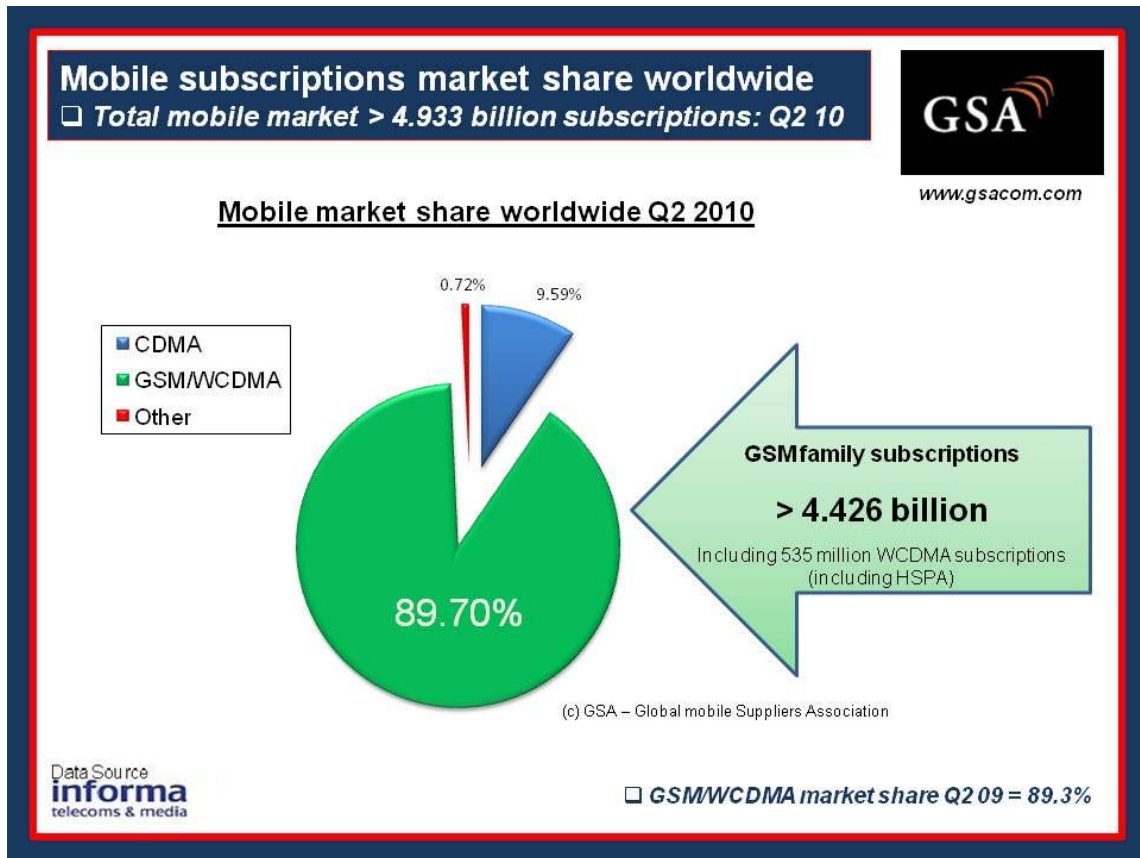


Figure 15. Mobile market share (From Global Mobile Suppliers Association, 2010)

### C. GSM NETWORK ARCHITECTURE

The general GSM network architecture is divided into three subsystems comprised of the following: mobile station, base station subsystem and the network subsystem as shown in Figure 16.

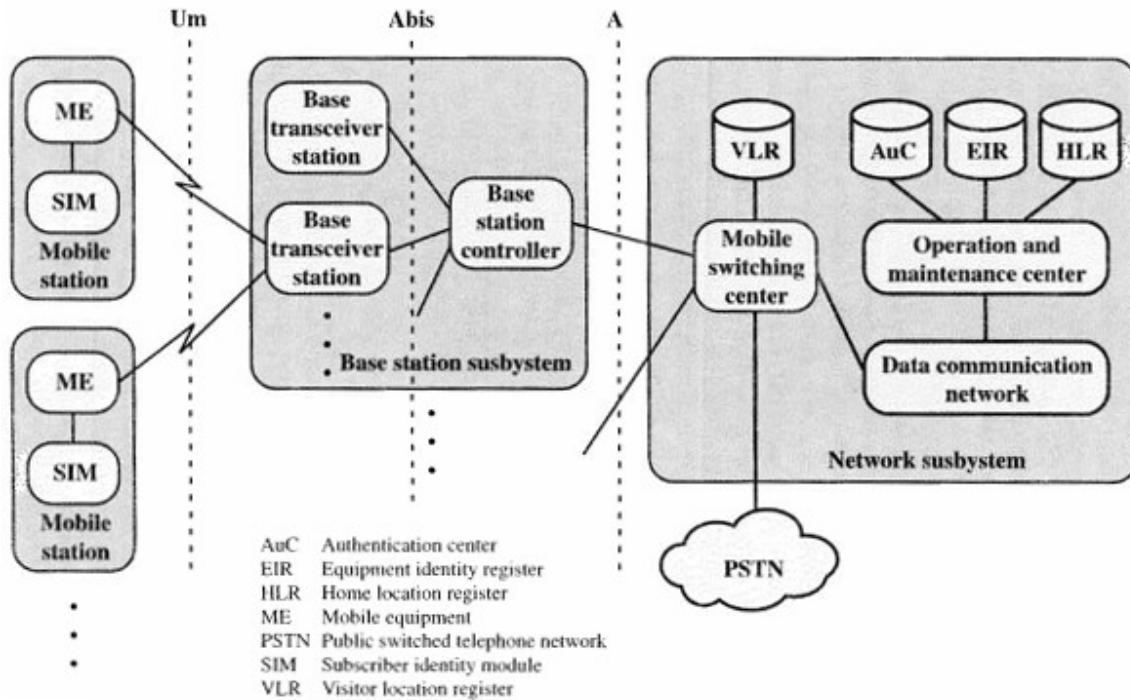


Figure 16. GSM architecture (From Stallings, 2005)

### 1. Mobile Station (MS)

The MS is comprised of the mobile equipment (ME) which is a subscriber's actual communications device or mobile phone. The ME is entirely generic until it is associated with a subscriber identity module (SIM), commonly referred to as a SIM card (Figure 17). The SIM contains the identifiers for the GSM network. The international mobile subscriber identity (IMSI) is embedded in the SIM and is used as the network identity for the subscriber (Figure 18). The ME also has an identifier for the hardware called the international mobile equipment identity (IMEI) (Stallings, 2005). The IMEI and IMSI are independent of each other and are both up to 15 digits in length. The IMSI is composed of the mobile country code (MCC) which identifies the country of the mobile network, the mobile network code (MNC) which is the specific mobile network in the country and the mobile subscriber identification number (MSIN) of the public land mobile network (PLMN) (Noldus, 2006). The MCC and MNC together identify the PLMN. An example would be 310 090 which is for AT&T in the United States (MCCLIST, 2012).



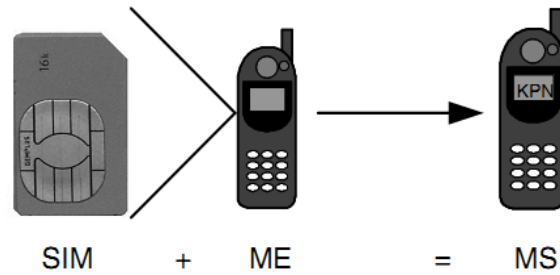


Figure 17. Components of mobile station (From Noldus, 2006)

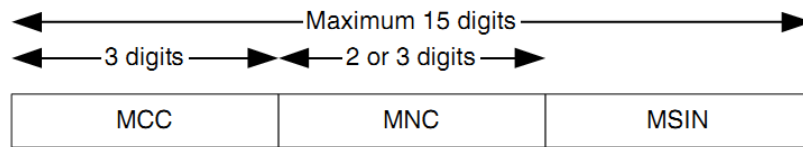


Figure 18. IMSI composition (From Noldus, 2006)

## 2. Base Station Subsystem (BSS)

The BSS consists of a base station controller (BSC) and one or more base transceiver stations (BTS).

### a. BSC

The BSC controls the resources of the BTS. “It handles the radio channel setup, frequency hopping and handover procedures when a user moves from one cell to another” (Bannister, Mather, & Coope, 2004). The BSC can be co-located with or linked to one or more BTSs either through a physical link such as a cable or a wireless microwave link (Figure 19).

### b. BTS

The BTS is what defines a cell in a cellular network; it contains the radio transceiver and antenna. A MS can only be connected to one BTS at a time. “In theory, a base station can cover an area with a radius of up to 35km” (Sauter, 2011), which is referred to as a cell. In different environments this area is drastically affected. The transmission power of the ME is typically between 1 and 2W which is the primary

limiting factor in the range of a cell. In urban environments the radius may be reduced to between 3 and 4km; while in rural areas coverage is typically less than 15km (Sauter, 2011).

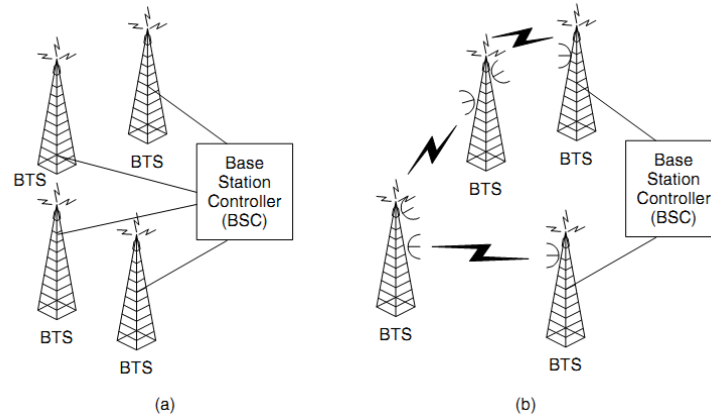


Figure 19. Base station subsystem: (a) wired, (b) wireless (From Bannister, Mather, & Coope, 2004)

### 3. Network Subsystem

The network subsystem is responsible for a number of things including “call establishment, call control and routing of calls between different fixed and mobile switching centers [...]” (Sauter, 2011). It is also what provides the link between the GSM network to other networks which could be a switched telephone network (PSTN), international fixed-line networks, other mobile networks, and Voice of Internet Protocol (VoIP) networks (Sauter, 2011). At the heart of the network subsystem is the mobile switching center (MSC) which interfaces with several databases.

#### *a. MSC*

The MSC takes care of both switching and what is called mobility management. When a MS is turned on and requests services from the mobile network, the MSC will process the request. The MSC will update the visitor location register (VLR) which will update the home location register (HLR) with the location of the MS within the network. The HLR may be located on another mobile carrier’s network if the MS has

roamed to a network that is not their home network. The MSC will also request information from the authentication center (AuC) about the subscriber in order to provide authentication and encryption services. The MSC will also monitor the connectivity between the BTS and the MS. The MSC will report a change of location update if the MS is no longer attached to the BTS (Bannister, Mather, & Coope, 2004).

***b. HLR***

The HLR is a critical subscriber database for a mobile network provider. The information stored for a subscriber in the HLR includes “their IMSI, service subscription information, service restrictions and supplementary services. The HLR is also expected to know the location of its mobile users” (Bannister, Mather, & Coope, 2004). The location of the MS is pulled from the VLR update.

***c. VLR***

The VLR database is temporary in nature and is usually integrated with an MSC. One of the main purposes of the VLR is to reduce the traffic to and from the MSC and the HLR. “When a subscriber leaves the coverage of an MSC, [their] record is copied from the HLR to the VLR of the new MSC, and is then removed from the VLR of the previous MSC” (Sauter, 2011).

**4. GSM Air Interface**

***a. Frequency Bands***

When GSM was standardized in Europe it was allowed to operate in the 900-MHz band, more specifically, between 890-MHz and 915-MHz for uplink (MS to BTS); and between 935-MHz and 960-MHz for downlink (BTS to MS). The bandwidth of each band is 25-MHz which is split into 125 channels. Each channel has a bandwidth of 200-kHz. When it became apparent that the portion of assigned spectrum was not going to be enough to support the growing user base, additional frequency ranges were assigned: 1710–1785-MHz (uplink) and 1805–1880-MHz (downlink). The bandwidth of each band was increased from 25-MHz to 75-MHz. Each channel remained at 200-kHz which resulted in 375 additional channels (Sauter, 2011). These two bands are

collectively referred to GSM900 and GSM1800. A graphical representation of GSM900 uplink channels 1–31 is shown in Figure 20.

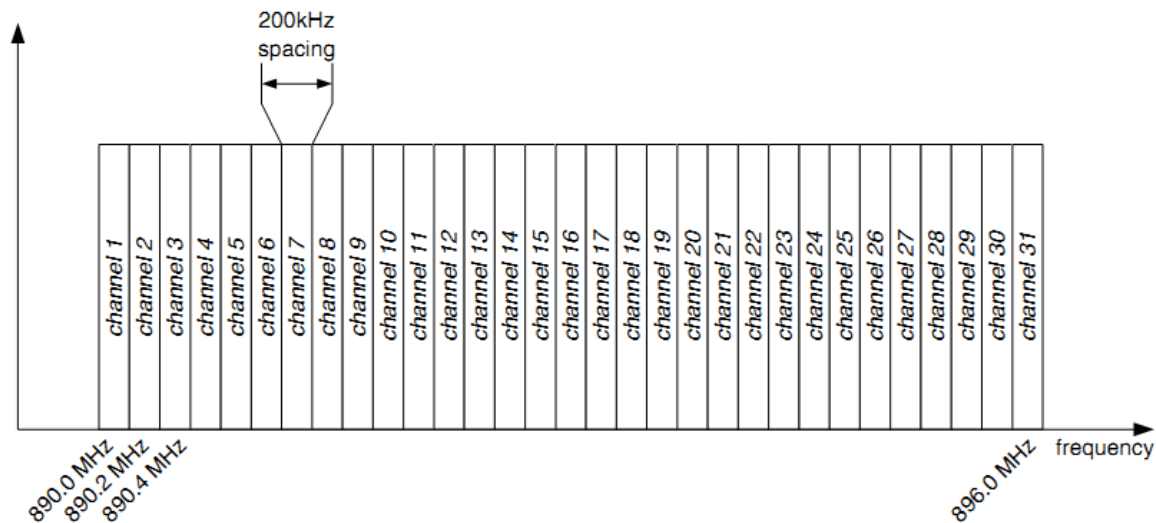


Figure 20. 200-kHz GSM uplink channels (From Bannister, Mather, & Coope, 2004)

When GSM was adopted in North America, the standard frequency bands being used in Europe were already allocated to other entities. In order to implement GSM, the North American regulating body chose to use frequency bands first in the 1900-MHz band and then eventually in the 850-MHz band (GSM1900 and GSM850) (Sauter, 2011).

***b. Absolute Radio Frequency Channel Numbers (ARFCN)***

ARFCNs are used to delineate a specific frequency to a channel within the bandwidth of the GSM uplink/downlink frequency range. Table 6 can be used to calculate uplink and downlink frequencies based on the associated AFRCN.

Table 6. ARFCNS and associated radio channels (From Telecom ABC, 2005)

Band	Name	ARFCN	Uplink(MHz)	Downlink(MHz)
GSM400	GSM400	$259 \leq n \leq 293$	$450.6 + 0.2 \times (n-259)$	$f_{up}(n) + 10$
		$306 \leq n \leq 340$	$479.0 + 0.2 \times (n-306)$	$f_{up}(n) + 10$
GSM700	GSM700	$438 \leq n \leq 511$	$747.2 + 0.2 \times (n-438)$	$f_{up}(n) + 30$
GSM850	GSM850	$128 \leq n \leq 251$	$824.2 + 0.2 \times (n-128)$	$f_{up}(n) + 45$
GSM900	Primary GSM	$1 \leq n \leq 124$	$890 + 0.2 \times n$	$f_{up}(n) + 45$
GSM900	Extended GSM	$0 \leq n \leq 124$ $975 \leq n \leq 1023$	$890 + 0.2 \times n$ $890 + 0.2 \times (n-1024)$	$f_{up}(n) + 45$
GSM900	GSM Rail	$0 \leq n \leq 124$ $955 \leq n \leq 1023$	$890 + 0.2 \times n$ $890 + 0.2 \times (n-1024)$	$f_{up}(n) + 45$
GSM1800	GSM1800 (DCS1800)	$512 \leq n \leq 885$	$1710.2 + 0.2 \times (n-512)$	$f_{up}(n) + 95$
GSM1900	GSM1900 (PCS1900)	$512 \leq n \leq 810$	$1850.2 + 0.2 \times (n-512)$	$f_{up}(n) + 80$

## 5. GSM Frames and Call Setup

In order to understand the GSM initial connection setup, it is important to understand the GSM framing. GSM uses frequency division multiplexing (FDM) to setup the RF channel(s) between the MS and the BTS (Figure 20). Time division multiplexing (TDM) is used for the traffic and control channels referred to as channel multiframes and hyperframes. The complex TDM hierarchy is shown in Figure 21.

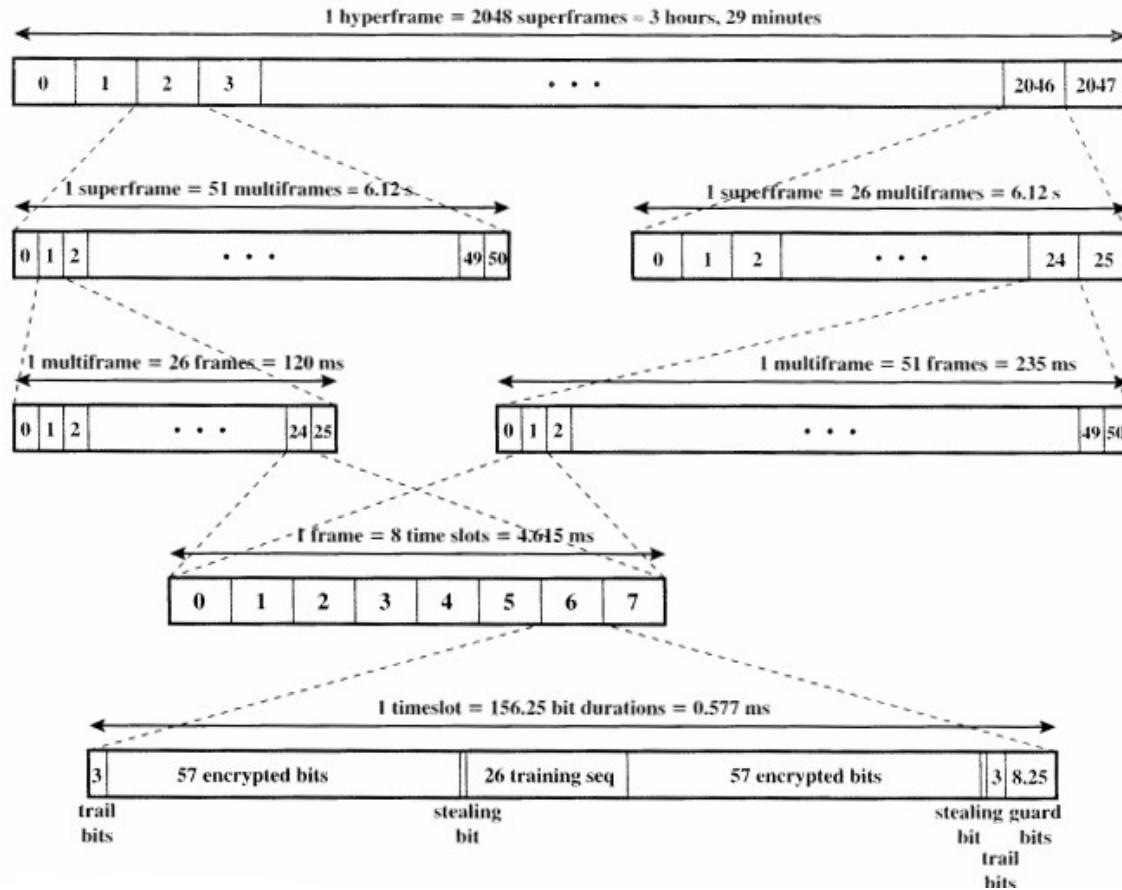


Figure 21. GSM TDM frame structure (From Stallings, 2005)

From Figure 21 it can be seen that there are two types of multiframe which make up superframes which in turn make up the hyperframe. “The traffic multiframe is comprised of 26 groups of 8 TDM frames while the control multiframe is comprised of 51 groups of frames” (Bannister, Mather, & Coope, 2004).

The timeslot is also referred to as a GSM burst and is divided up into different sections as shown in Figure 21. The guard bits are where no data is sent. This is necessary because a MS might change their distance to the BTS during an active call. Since the RF signal is bound by traveling at the speed of light, it may take a signal longer to reach the BTS. The guard bits help prevent overlap (Sauter, 2011).

The training sequence always contains the same bit pattern. It is used to help the receiver compensate for interference that may be induced from reflection, absorption and multipath propagation (Sauter, 2011).

The trail bits are used to inform the receiver of the beginning and end of the GSM burst (timeslot).

The stealing bits are used to let the network know if the user data (57 encrypted bits) is going to be “stolen” and urgent signaling data is passed instead. User data is lost in this case; however, because of the short time duration it should be nearly transparent to the subscriber.

#### ***a. Control Channel Multiframe***

The control channel multiframe is responsible for control, timing and signaling. The logical channels are described below:

- Broadcast Channel (BCCH) – The main information channel of a cell which broadcasts information about the network and contains the MCC, MNC and location area code (LAC) of the BTS. All MS monitor BCCH for BTS identity and channel status (Sauter, 2011).
- Frequency Correction Channel (FCCH) – Used to keep the MS locked onto the frequency reference of the BTS so that it does not drift off, which would result in reduced signal quality of a call (Bannister, Mather, & Coope, 2004).
- Synchronization Control Channel (SCH) – Used to synchronize the frames with a MS (Bannister, Mather, & Coope, 2004).
- Random Access Channel (RACH) - This channel is part of the uplink direction. It allows a MS to request a dedicated control channel with which to establish communications on. Channel assignment is random in nature so that two MS will not try to establish a connection on the same channel. If this occurs it is called a collision and the messages are lost. The MS will have to initiate another RACH request after a period of time (Sauter, 2011).
- Paging Channel (PCH) – Used to inform MS of an incoming call or SMS messages. The network will use a subscriber’s IMSI or temporary mobile subscriber identity (TMSI) in order to identify the MS that the inbound message is assigned to. TMSIs are utilized to prevent the network from broadcasting a subscriber’s IMSI unnecessarily. An MS is assigned a TMSI when it first attaches to the network (Sauter, 2011).

- Standalone Dedicated Control Channel (SDCCH) – Utilized when a subscriber has not yet been assigned a dedicated traffic channel. This channel helps conserve bandwidth on the network. It is used to pass location updates of the MS and SMS messages where dedicated voice channels are not required (Bannister, Mather, & Coope, 2004).
- Slow Associated Control Channel (SACCH) – Used to pass signal quality to and from the network. The network will use this information for handover determination and power control (Sauter, 2011).
- Fast Associated Control Channel (FACCH) – The channel will interrupt user data to quickly pass information to the network such as parameters required for a handover (Sauter, 2011).

***b. Traffic Channel Multiframe***

As previously mentioned, the traffic channel multiframe consists of 26 frames where only 24 are used for dedicated user data (TCH). Frames 12 and 25 are assigned to be used as SACCH (as described in the previous section). SMS messages can be transferred to and from the MS using the SACCH if a call is in progress. The TCH may be interrupted by a FACCH if a handover within the network is necessary (Bannister, Mather, & Coope, 2004).

A detailed diagram depicting the timeslots in both the control and traffic channels in the downlink is shown in Figure 22.



FN	TS-0	TS-1	FN	TS-2	TS-7
0	FCCH	SDCCH/0	0	TCH	TCH
1	SCH	SDCCH/0	1	TCH	TCH
2	BCCH	SDCCH/0	2	TCH	TCH
3	BCCH	SDCCH/0	3	TCH	TCH
4	BCCH	SDCCH/1	4	TCH	TCH
5	BCCH	SDCCH/1	5	TCH	TCH
6	AGCH/PCH	SDCCH/1	6	TCH	TCH
7	AGCH/PCH	SDCCH/1	7	TCH	TCH
8	AGCH/PCH	SDCCH/2	8	TCH	TCH
9	AGCH/PCH	SDCCH/2	9	TCH	TCH
10	FCCH	SDCCH/2	10	TCH	TCH
11	SCH	SDCCH/2	11	TCH	TCH
12	AGCH/PCH	SDCCH/3	12	SACCH	SACCH
13	AGCH/PCH	SDCCH/3	13	TCH	TCH
14	AGCH/PCH	SDCCH/3	14	TCH	TCH
15	AGCH/PCH	SDCCH/3	15	TCH	TCH
16	AGCH/PCH	SDCCH/4	16	TCH	TCH
17	AGCH/PCH	SDCCH/4	17	TCH	TCH
18	AGCH/PCH	SDCCH/4	18	TCH	TCH
19	AGCH/PCH	SDCCH/4	19	TCH	TCH
20	FCCH	SDCCH/5	20	TCH	TCH
21	SCH	SDCCH/5	21	TCH	TCH
22	SDCCH/0	SDCCH/5	22	TCH	TCH
23	SDCCH/0	SDCCH/5	23	TCH	TCH
24	SDCCH/0	SDCCH/6	24	TCH	TCH
25	SDCCH/0	SDCCH/6	25	Free	Free
26	SDCCH/1	SDCCH/6	0	TCH	TCH
27	SDCCH/1	SDCCH/6	1	TCH	TCH
28	SDCCH/1	SDCCH/7	2	TCH	TCH
29	SDCCH/1	SDCCH/7	3	TCH	TCH
30	FCCH	SDCCH/7	4	TCH	TCH
31	SCH	SDCCH/7	5	TCH	TCH
32	SDCCH/2	SACCH/0	6	TCH	TCH
33	SDCCH/2	SACCH/0	7	TCH	TCH
34	SDCCH/2	SACCH/0	8	TCH	TCH
35	SDCCH/2	SACCH/0	9	TCH	TCH
36	SDCCH/3	SACCH/1	10	TCH	TCH
37	SDCCH/3	SACCH/1	11	TCH	TCH
38	SDCCH/3	SACCH/1	12	SACCH	SACCH
39	SDCCH/3	SACCH/1	13	TCH	TCH
40	FCCH	SACCH/2	14	TCH	TCH
41	SCH	SACCH/2	15	TCH	TCH
42	SACCH/0	SACCH/2	16	TCH	TCH
43	SACCH/0	SACCH/2	17	TCH	TCH
44	SACCH/0	SACCH/3	18	TCH	TCH
45	SACCH/0	SACCH/3	19	TCH	TCH
46	SACCH/1	SACCH/3	20	TCH	TCH
47	SACCH/1	SACCH/3	21	TCH	TCH
48	SACCH/1	Free	22	TCH	TCH
49	SACCH/1	Free	23	TCH	TCH
50	Free	Free	24	TCH	TCH
			25	Free	Free

Figure 22. Timeslot in the downlink direction (From Sauter, 2011)

*c. Initial Connection Process*

Once the MS is initially turned on it will search for a strong BCCH signal. Once it selects a strong BCCH it will attempt to register with the network. When it attempts to register with the network it sends a RACH request. The network will respond on the access grant channel (AGCH) and further network transactions will occur over the SDCCH. The MS's SIM card IMSI will be sent to the MSC for authentication. The MSC will connect to the HLR of the MS's home network. After the SIM is authenticated, the MSC will request the IMEI to verify it against the equipment identity register (EIR) which is a list of valid devices on a network. If the IMEI is determined not valid, the MS will not be allowed to register to the network. Once the IMSI and IMEI have been validated, the MSC will register the MS with the VLR and assign it a TMSI for future use. Once the initial connection process is complete (Figure 23) the MS will be assigned either a SDCCH or a TCH (Bannister, Mather, & Coope, 2004).

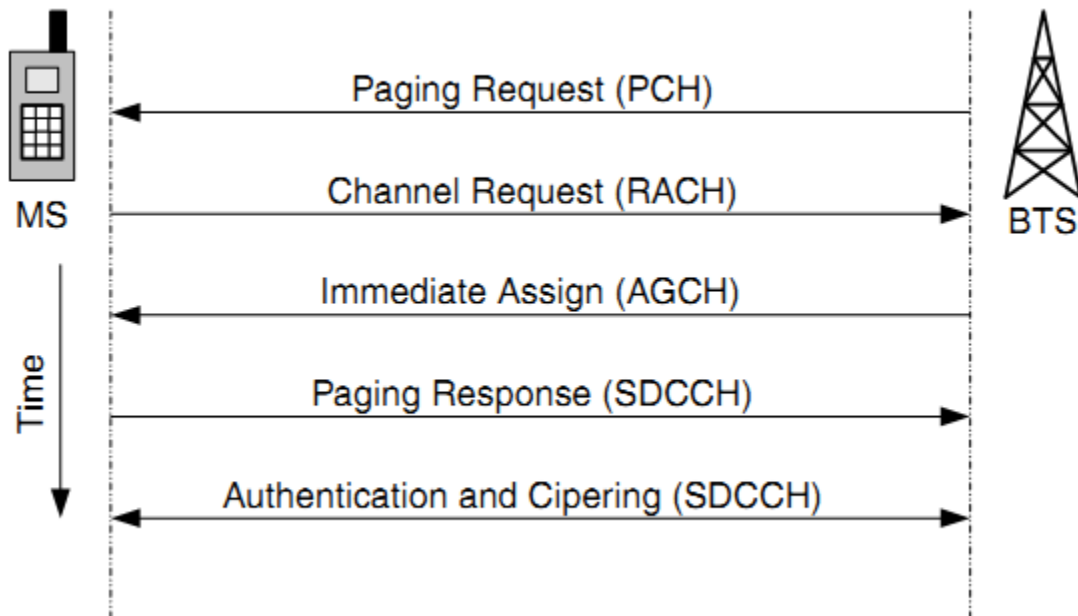


Figure 23. Initial connection process (From Bannister, Mather, & Coope, 2004)

***d. Follow-On Connections***

After a MS has been authenticated on the GSM network, the rest of the call connecting process is handled by signaling system 7 (SS7). SS7 is an international signaling system standardized by the International Telecommunications Union Telecommunications Standardization Sector (ITU-T). The USA uses a similar SS7 standardized by the American National Standards Institute (ANSI). SS7 has proven to be a reliable system due to stringent requirements as stipulated by the ITU-T outlined in their Q-Series Recommendation publications (Bannister, Mather, & Coope, 2004).

An example SS7 network is shown in Figure 24. The network is made up of three primary nodes: service switching points (SSP), signal transfer points (STP) and service control points (SCP). Multiple links connect the nodes to ensure reliability. Commencing, addressing and aborting a call to a destination is the responsibility of the SSP (MSC in a GSM network). STP provides a path from source to destination similar to a router in TCP/IP networks. The SCP is required when an alias instead of a destination number is used (Bannister, Mather, & Coope, 2004). An example is in the case of toll-free numbers where the 1-800 number is not the actual destination number. From Figure 24, User A would dial a 1-800 number for User B, but the 1-800 number is not User B's actual termination point. The SCP would provide the destination number that correlates with the 1-800 number User A dialed, which would then be routed accordingly.

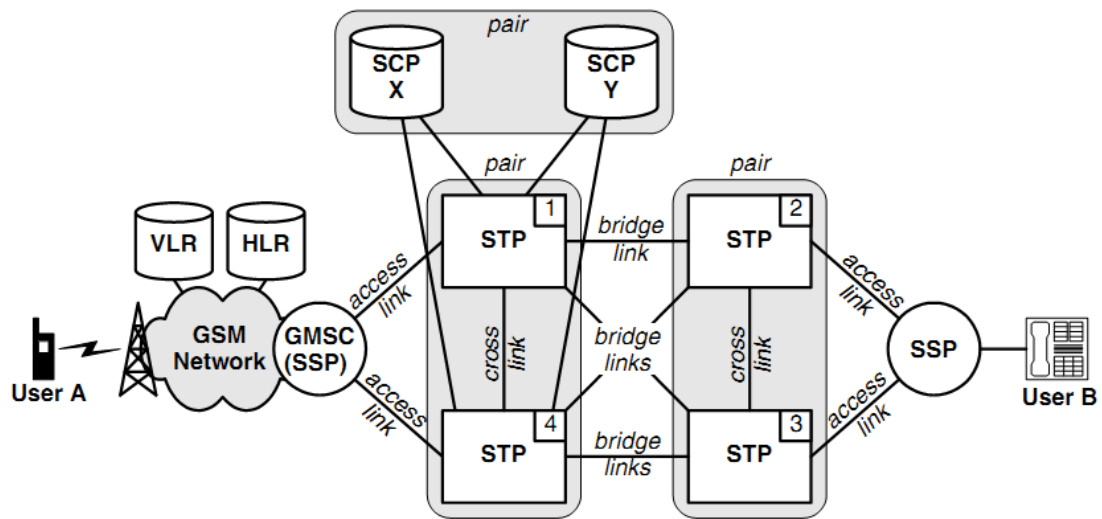


Figure 24. SS7 network (From Bannister, Mather, & Coope, 2004)

## **IV. SOFTWARE-DEFINED RADIO (SDR)**

### **A. INTRODUCTION**

In order to understand how to implement GSM with standard radio frequency (RF) hardware, it is necessary to cover the software that will interface with the hardware to create such a system. This chapter takes a brief look at software-defined radio (SDR), its background, basic architecture, concepts, and its evolution in commercial and military systems. This chapter also explores currently available commercial-off-the-shelf system used for rapid prototyping and research. Basic architecture and concepts of SDR are discussed as well.

### **B. BACKGROUND**

The Wireless Innovation Forum (formerly known as the SDR Forum) defines SDR as a “radio in which some or all of the physical layer functions are software defined” (Wireless Innovation Forum, 2012). SDR relies heavily on computer architectures and processing capability. Prior to the 1980s, the processing power required to do traditional RF processing was not as accessible. When processing power started to become more accessible, developments in SDR started to become more feasible. E-Systems (now part of Raytheon) published a report in 1985, “New Research Lab Leads to Unique Radio Receiver,” which stated:

A group of Garland E-Teamers had to create an ultra-fast data processor, configured as a digital radio receiver, because their large general purpose computer was too slow to run a promising new radio signal processing technique being developed in an R&D project. [People] who have seen it, all agree that the new digital computer based receiver, called Software Radio, has the potential to revolutionize the field of processing very complex radio signals. (E-Sytems, 1985)

The slight change from E-Systems’ term, “software radio” to “software-defined radio” came in 1991 from Dr. Joseph Mitola who went on to serve as Vice President for The Research Enterprise at Stevens Institute of Technology (Schaefer School of Engineering & Science, 2010).

### **C. COMMERCIAL COMMUNICATIONS USE**

The benefits of SDR for commercial enterprise usage can be quite appealing, especially with the rapid changes in communications technology that have been observed over the last two decades. A SDR has the capability to provide an adaptable architecture that allows changing of a radio's characteristics nearly on-the-fly. For commercial vendors and providers of mobile communications, this flexible architecture allows for easier upgrades to infrastructure and to get new services out to the market as the demand arises. Some examples of upgrades that are implemented using SDR may be "interference rejection techniques, encryption, voice recognition and compression, software-enabled power minimization and control, different addressing protocols, and advanced error recovery schemes" (Reed, 2002). SDR has made it possible for wireless service providers to keep up with the evolving mobile protocols (2G, 2.5G, 3G, 4G, etc.). Without SDRs, wireless service providers would have spent a significant amount of capital replacing their entire infrastructure every several years (Reed, 2002).

### **D. MILITARY COMMUNICATIONS USE**

With the adaptive capability that SDR has, it brings a number of benefits to military units, especially in joint and coalition environments where units will find themselves trying to carry out operations with various communications standards. SDR allows quick reconfiguration of the radios in order for the units to communicate with each other.

Starting in 1990, the U.S. Military began a program called SPEAKeasy to start implementing SDR into the communications architecture. SPEAKeasy phase 1 was primarily a proof of concept. The form factor was large and required an entire rack of equipment, which made it not quite portable, thus limiting the system to bases or ships. Man-portable form factors and airplane deployable versions weren't available until SPEAKeasy phase 2 was introduced in 1997. The form factor evolution from large-scale to man-portable is illustrated in Figure 25.

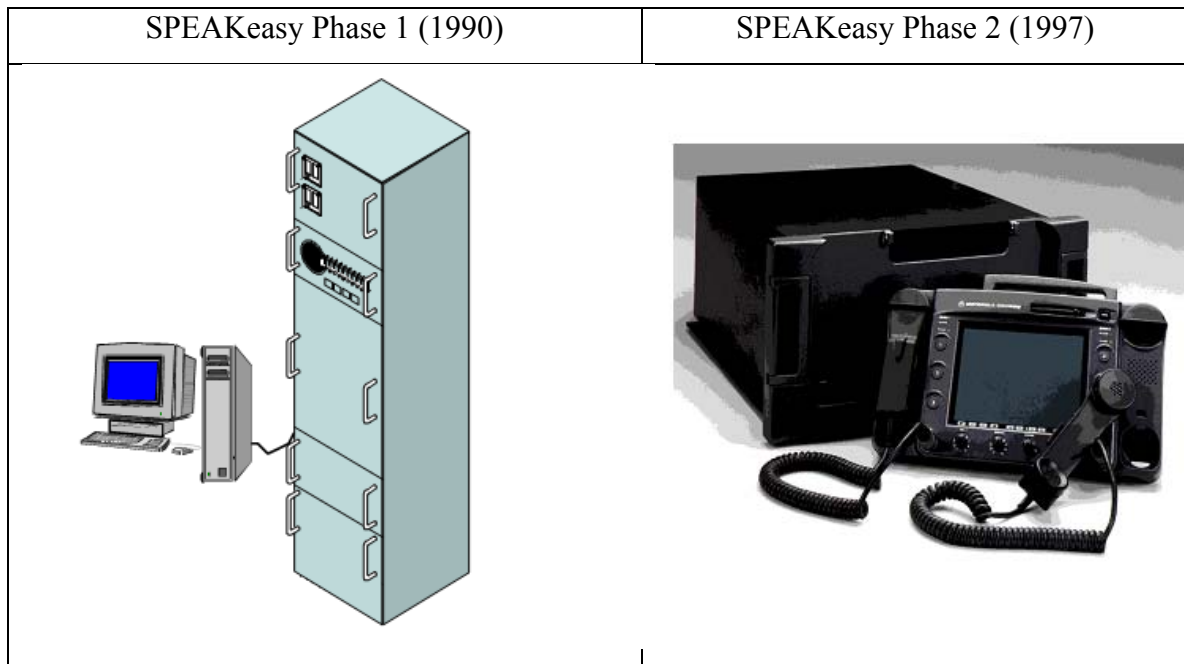


Figure 25. SPEAKeasy form factors (From Bonsor, 1998)

The SPEAKeasy program was followed by a new program development in 1998 called the Joint Tactical Radio System (JTRS) which is the program of record still in use today (Nathans & Stephens, 2007).

#### **E. SDR ARCHITECTURE**

A comparison of a traditional analog receiver chain to a SDR receiver chain is showing in Figure 26. The RF-to-intermediate frequency (IF) and analog-to-digital conversions take place in the RF frontend before being processed by a SDR.

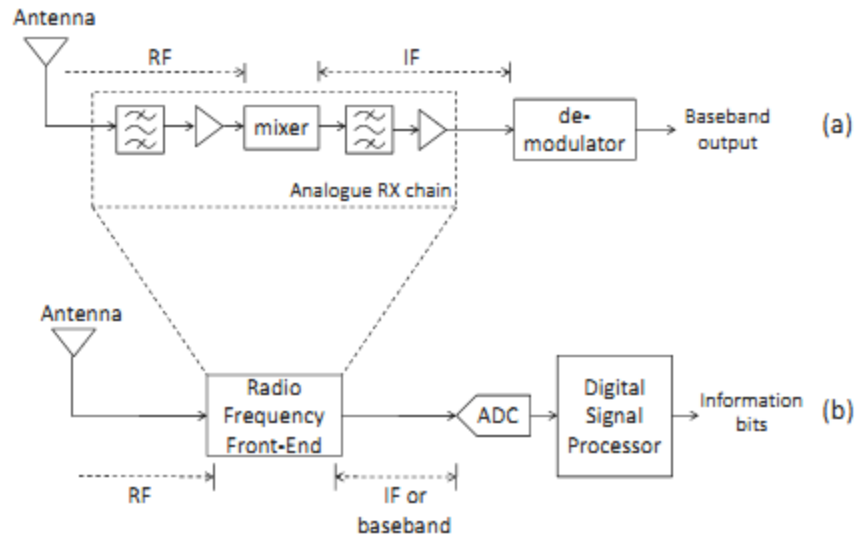


Figure 26. Analog (a) and digital (b) hardware receivers (From Valerio, 2008)

A SDR, while “software defined,” won’t be able to do much without a hardware interface which is usually referred to as the “RF frontend” where the analog signal is taken from the radio frequency spectrum and converted into the digital domain.

A high-level functional model of the SDR consists of only three main elements: analog front-end, the domain conversion and the digital processing backend (Figure 27). Properties of the domain converters both analog-to-digital (ADC) and digital-to-analog (DAC) heavily influence the functionality of the SDR platform (Eged & Babjak, 2006).

Limitations at the RF frontend include type of antenna and down conversion. Future developments and research include adaptable RF frontends which will configure themselves for whatever RF environments they may be in. Frontend architecture may also include amplifiers, especially, if the SDR is intended to transmit.



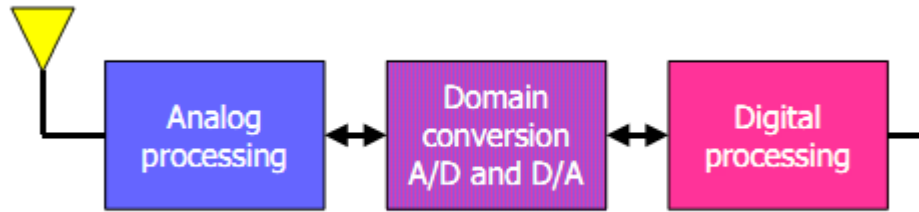


Figure 27. SDR-based radio implementation (From Eged & Babjak, 2006)

SDR technology is based on the principle that the domain conversion (analog and digital domains) should take place as close to the antenna as possible, thus maintaining the signal in the digital domain (Eged & Babjak, 2006) as long as possible. There are various implementation levels of handling an RF signal in the analog and digital domains (Figure 28). Depending on the signal type and the capability of the SDR, it may not be possible for the analog-to-digital conversion to take place at the antenna. In the case of higher frequency signals, a much faster ADC or DAC will be required. Hardware may have to convert the RF signal to an acceptable IF for the SDR platform to handle. Among other factors that will have to be taken into consideration will be the signal's bandwidth.

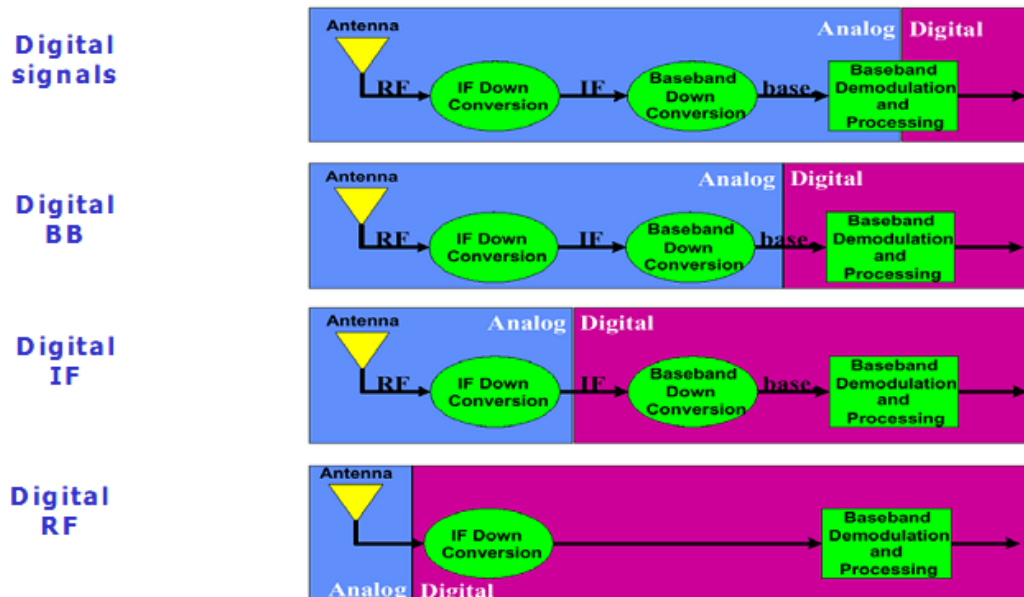
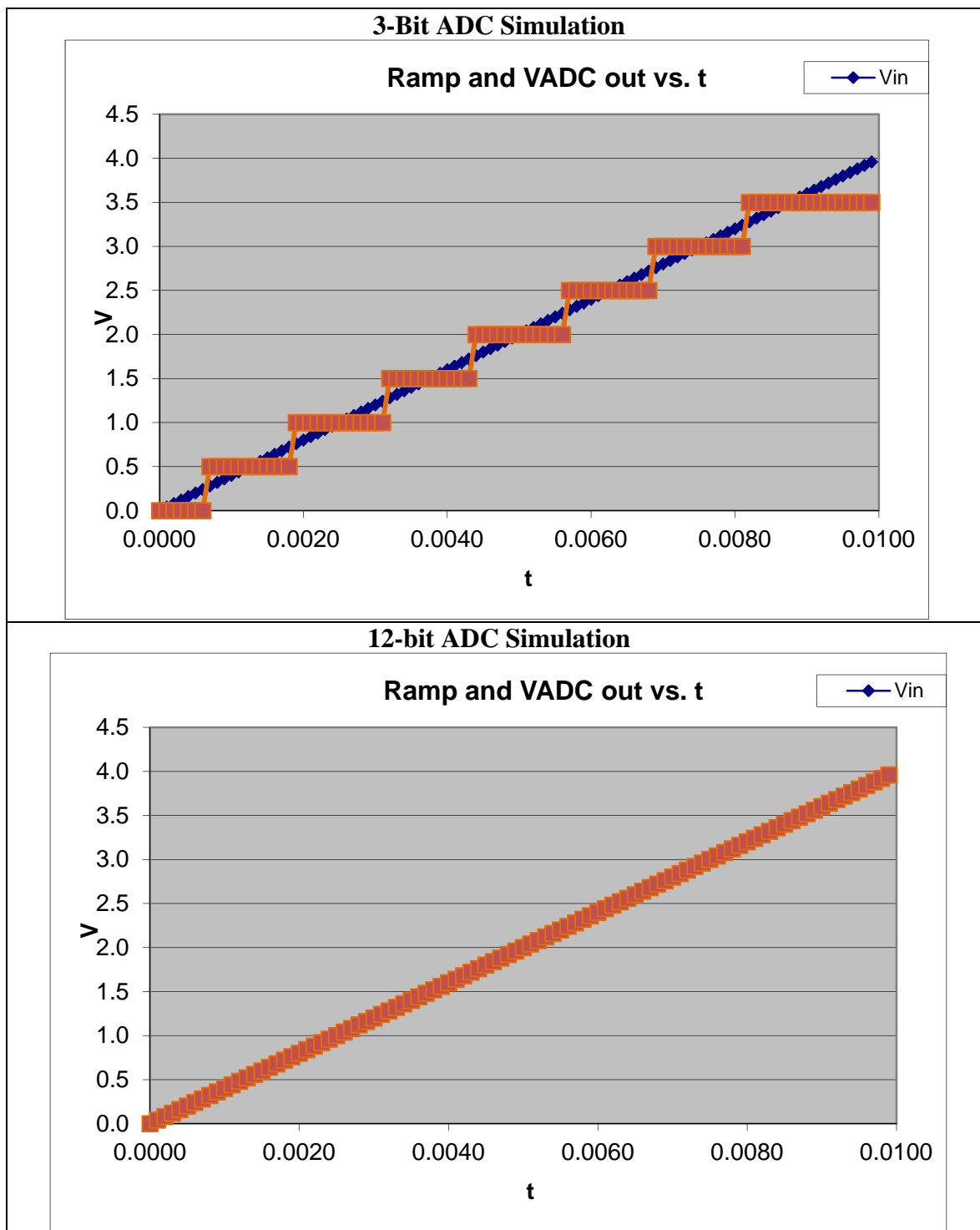


Figure 28. SDR implementation levels (From Eged & Babjak, 2006)

## **1. ADC**

The analog-to-digital converter is one of the core components of SDR. This is where the signal in the RF spectrum is converted into the digital domain and the bits can be further processed. Amplitude Quantizing is the task of mapping samples of a continuous amplitude waveform to a finite set of amplitudes. The keyword here is ‘finite.’ The ADC is the hardware that performs this mapping. ADC resolution and sampling rate are important factors to take into account when evaluating an ADC. Determining what types of signals-of-interest (SOIs) the SDR is designed for will drive the parameters for the ADC choice. A comparison of a 3-bit ADC to a 12-bit ADC is shown in Table 7. The analog signal is the ramp (0–4V) of a saw tooth wave and the ADC output is superimposed over the ramp of the saw tooth wave. The, 3-bit ADC represents the slope of the saw tooth wave in a staircase-like fashion which is quite poor. With an increase to 12-bit ADC the representation is nearly the same for digital and analog slopes.

Table 7. ADC Resolution 3-bit to 12-bit comparison



In order to determine the resolution of the ADC, a determination of the quantization step is required. The following equation is used for this calculation:

$$q = \frac{2E_{\max}}{2^b} \quad (0.1)$$

Where  $E_{\max} = \pm$  range of signal in volts. For the signal represented in Table 4, the value would be 2.0V normalized and  $b$  is the number of bits used in the conversion process. The smaller the value of  $q$  (also called the quantizing step or quantile), the higher the resolution ADC (Sklar, 2001).

The ADC is the entry point of a RF signal into an SDR system and it can also be a single point of failure if not matched correctly to what the system is intended to achieve.

## **2. The Universal Software Radio Peripheral**

The Universal Software Radio Peripheral (USRP) is an instrument developed by Ettus Research, LLC, which allows a general purpose computer to be used as a flexible SDR platform for research and prototyping. Ettus Research offers three different lines of USRPs. A bus series which is interfaced locally using a USB2 connection; a networked series which allows remote interface via Ethernet connection. Finally, an embedded series which has a computer embedded into the device that can be interfaced either remotely via a network connection or locally with a keyboard, monitor and mouse. A simplified schematic of a two channel bus series USRP is shown in Figure 29.

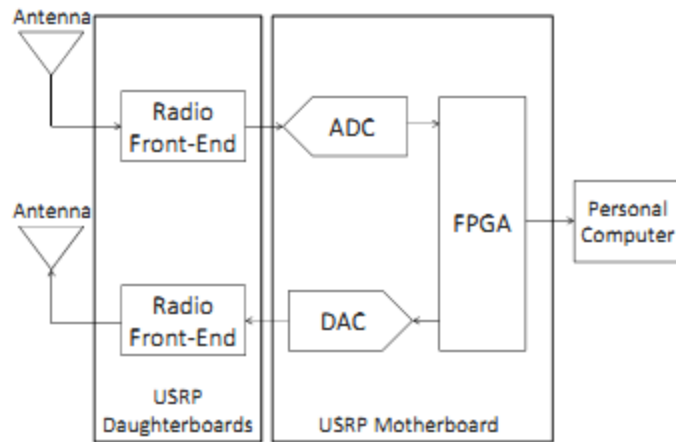


Figure 29. USRP simplified block diagram (From Valerio, 2008)

The USRP motherboard contains up to four high-speed ADCs and DACs (just two are illustrated in Figure 29), a field programmable gate array (FPGA), and up to four daughterboards, which act as the radio frontend. The FPGA is responsible for high speed general purpose processing like up and down conversion, filtering, sampling and interpolation. The FPGA is connected to the general purpose computer by either a USB2, gigabit Ethernet or embedded interface. The general purpose CPU is responsible for wave-form specific processing such as modulation and demodulation (Valerio, 2008). Ettus Research offers six different models of USRPs. A comparison of the specific parameters for each model is shown in Table 8. The Ettus N-series is the networked USRP line, the E-series is the embedded line and the B-series is the USB line. A list of available daughterboards available for use with the USRP is shown in Table 9.

Table 8. USRP parameters (From Ettus Research LLC, 2012)

Model	RF Channels	Host Interface	DAC	ADC	CPU
N200	1TX/1RX	GigE	16-bit, 400MSPS	14-bit, 100MSPS	n/a
N210	1TX/1RX	GigE	16-bit, 400MSPS	14-bit, 100MSPS	n/a
E100	1TX/1RX	Embedded	14-bit, 128MSPS	12-bit, 64MSPS	OMAP3730
E110	1TX/1RX	Embedded	14-bit, 128MSPS	12-bit, 64MSPS	OMAP3730
USRP1	2TX/2RX	USB 2.0	14-bit, 128MSPS	12-bit, 64MSPS	n/a
B100	1TX/1RX	USB 2.0	14-bit, 128MSPS	12-bit, 64MSPS	n/a

Table 9. Available daughterboards (From Ettus Research, LLC, 2012)

Name	Frequency Range and Description
• BasicRX	1–250MHz Receive
• BasicTX	1–250MHz Transmit
• LFRX	0–30MHz Receive
• LFTX	0–30MHz Transmit
• TVRX2	Dual 50–860MHz Receive
• DBSRX2	800–2350MHz Receive
• RFX900	800–1000MHz Transceiver
• RFX1200	1150–1400MHz Transceiver
• RFX1800	1500–2100MHz Transceiver
• RFX2400	2300–2900MHz Transceiver
• XCVR2450	2400–2500MHz & 4900–5850MHz Dual-band Transceiver
• WBX	50–2200MHz Transceiver
• SBX	400–4400MHz Transceiver

The Basic RX/TX boards do not have any mixer, filter, or amplifier. They merely act as interface between the USRP and the RF spectrum. The RFX series offers a complete RF transceiver with local oscillators and transmit/receive switches (Valerio, 2008).

### 3. Software: GNU Radio

After the USRP is configured and connected to a general computing platform running a Linux Operating System, software is required to manipulate the stream of bits which are coming through the host interface connection. While there are many software suites available, GNU Radio is freely available and is widely used to interface with USRPs. “GNU Radio is a free software development toolkit that provides the signal processing runtime and processing blocks to implement software radios using readily-available, low-cost external RF hardware and commodity processors” (GNU Radio, 2012). GNU Radio offers an extensive list of modules used for signal processing and graphical display as shown in Table 10.

Table 10. List of GNU Radio modules (From Valerio, 2008)

GNU Radio Modules
<ul style="list-style-type: none"><li>• Mathematical operations (add, multiply, log, etc.)</li><li>• Interleaving, delay blocks, etc.</li><li>• Filters (Finite Impulse Response, Infinite Impulse Response, Hilbert, etc.)</li><li>• FFT blocks</li><li>• Automatic Gain Control (AGC ) blocks</li><li>• Modulation and demodulation (FM, AM, PSK, QA M, GMSK, OFDM, etc.)</li><li>• Interpolation and decimation</li><li>• Trellis and Viterbi support</li><li>• Signal generators</li><li>• Noise generators</li><li>• Pseudorandom number generators</li><li>• USRP source and sink (to transmit/receive signal via USRP)</li><li>• Graphical sinks (Oscilloscope, FFT, etc.)</li><li>• Audio source and sink</li><li>• File source and sing (reads/writes samples from/to a file</li><li>• User Datagram Protocol (UDP) source and sink (to transport samples over a network)</li></ul>

The GNU Radio graphical user interface (GUI) with modules set up to receive a signal source via the computer's sound card (sampled at 44.1kHz) and display the signal in both the time and frequency domains is shown in Figure 30.

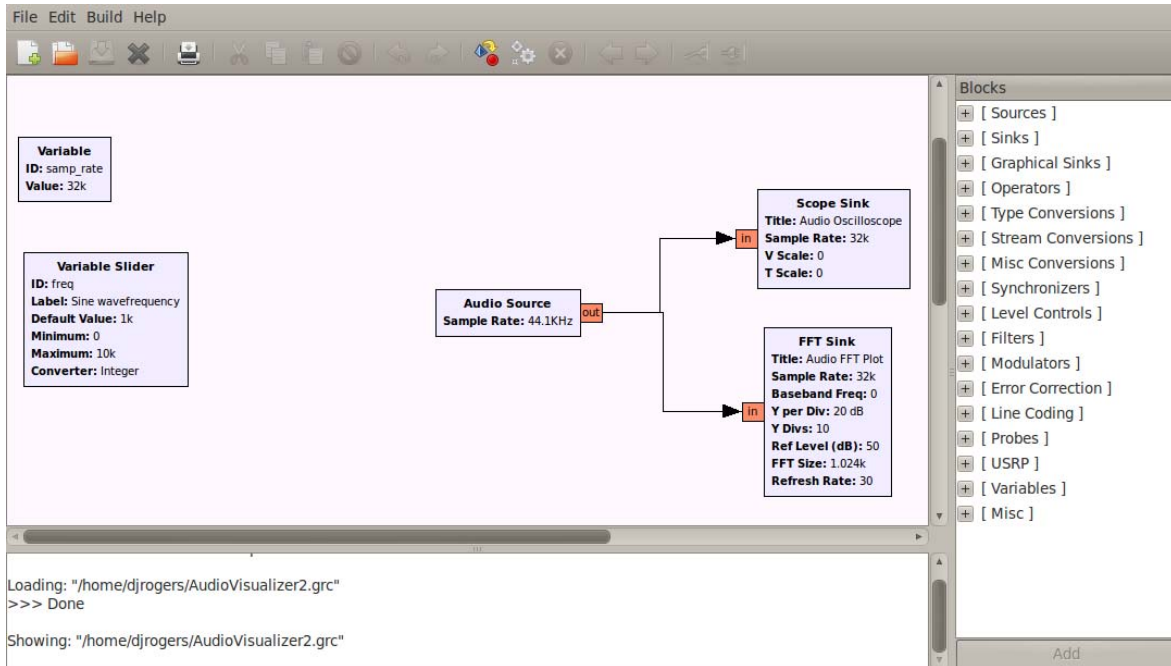


Figure 30. GNU Radio GUI

A 1kHz sine wave (generated using a tone generator), displayed in both the GNU Radio FFT and oscilloscope plots is shown in in Figure 31. X-axis for the FFT plot is in 20 dB/div while the y-axis is in kHz.



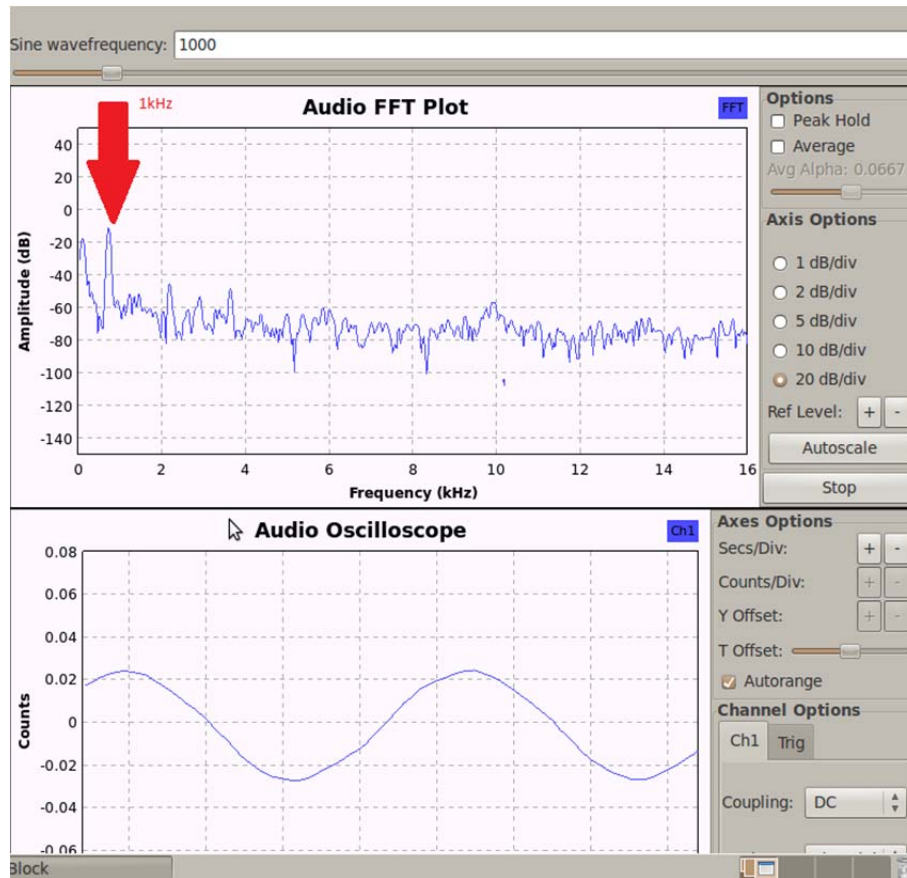


Figure 31. GNU Radio oscilloscope and FFT plots

## F. SUMMARY

SDR offers a lot of flexibility for interfacing with the RF spectrum. Technology developments have offered affordable open-source platforms for researchers to experiment and develop with. The same technology is also available to adversaries which can be used for devious activities. Affordable processing power will enable people to build communications or SIGINT systems they might not previously have been able to afford or have the skills required to maintain.

Most “smart phones” are actually small computing platforms capable of running a SDR. Having a SDR on the communications device enables a highly configurable and adaptable platform where the biggest adjustment would actually be changing hardware, such as the antenna, in order to adapt to whatever frequency environment the SDR is required to operate in.

THIS PAGE INTENTIONALLY LEFT BLANK

## V. SMALL FORM FACTOR GSM SYSTEM

### A. INTRODUCTION

This chapter will discuss the hardware and software used to build a small form factor GSM system which will be capable of being deployed on a SUAS. It will also discuss test results on the ground and at altitude. A system overview and comparison to the traditional GSM network is shown in Figure 32. In the small form factor GSM system, the hardware (USRP) will contain an integrated processor which will run the required software.

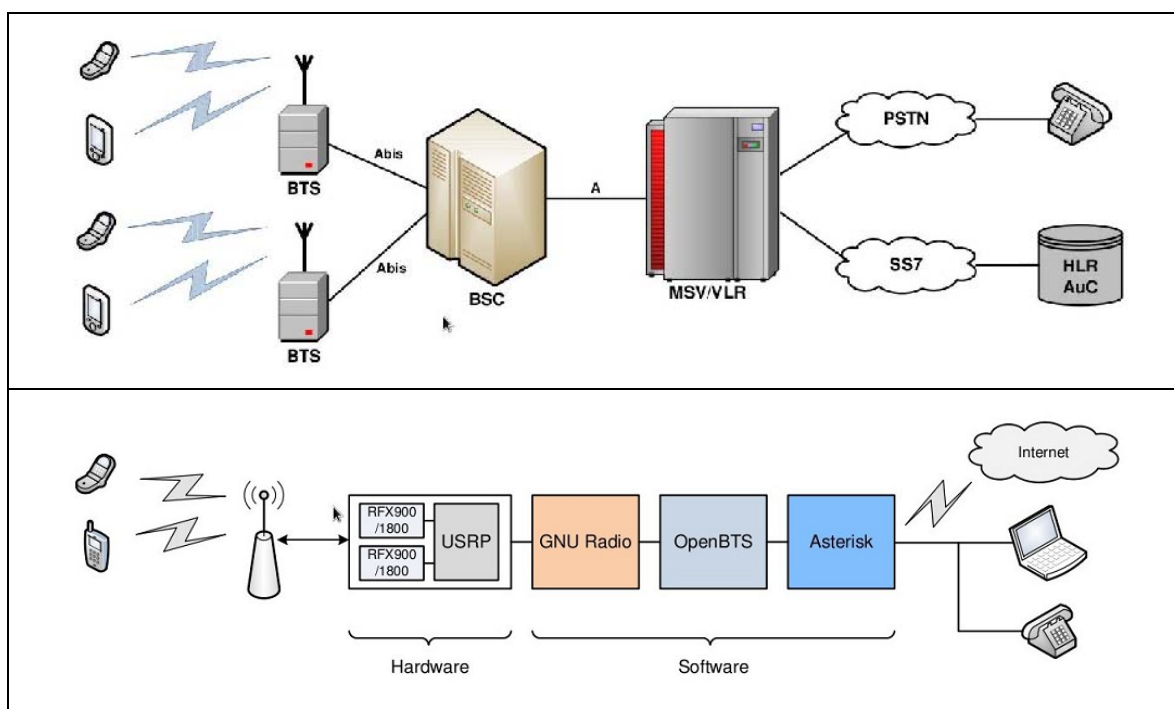


Figure 32. Traditional GSM network (top), notional OpenBTS network (bottom)  
(From Spicer, 2010)

### B. HARDWARE

#### 1. USRP Ettus Research E100 SDR System

The Ettus Research E100 USRP model was chosen due to its availability and its integrated computing capability. It is an all-in-one unit with a FPGA and a computer-on-

module (COM). It was critical in finding a computing platform where there would be no traditional hard drive storage with spinning platters due to the nature of vibrations the hardware would encounter onboard a UAS (Garcia & Valavanis, 2007). The E100 also has a temperature compensated crystal oscillator (TCXO) which can be adjusted. The TCXO allows for changes in the hardware clock without having to install a separate oscillator to achieve timing changes. The E100 can be interfaced locally using keyboard, video and mouse. The video output is through a high-definition multimedia interface (HDMI) connection. The keyboard and mouse need a powered USB hub in order to be connected to the E100. Once the initial system configuration is complete, there is no longer a need to interface with the unit locally and it can be interfaced with through a network connection. Network connectivity is provided by a standard Ethernet connection. A functional block diagram is shown in Figure 33.

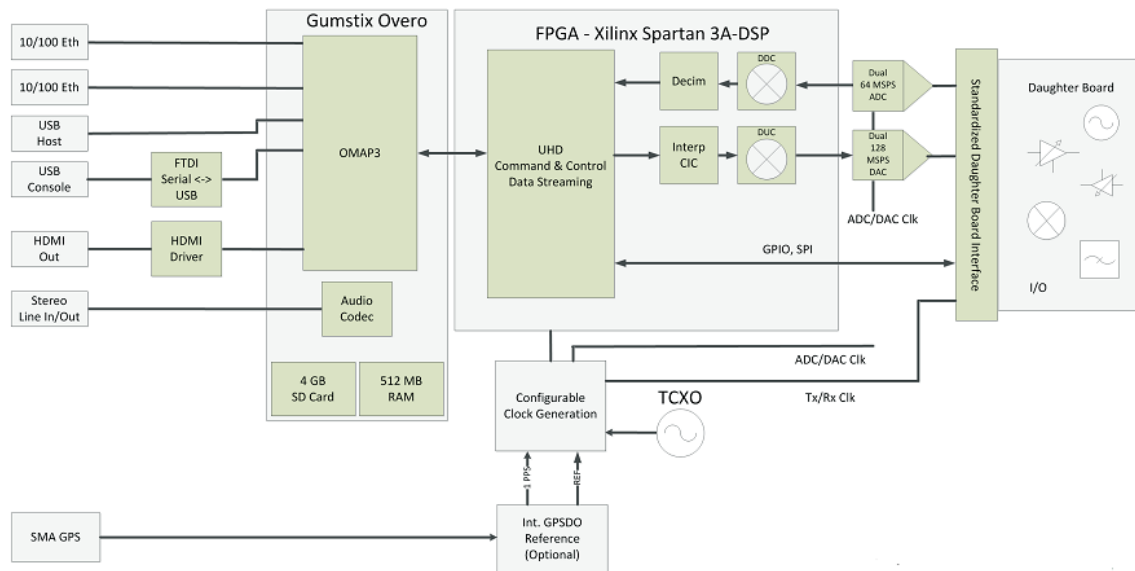


Figure 33. Ettus Research USRP E100 block diagram (From Ettus Research LLC, 2012)

The E100 supports one TX/RX daughter board. The RFX900 was chosen due to its frequency range of 750–1050MHz, which will cover the GSM850 and GSM900 bands. The typical power output of the RFX900 is 200mW. Standard Ettus Research

VERT900 omni-directional antennas were used to connect to the transmit and receive interfaces on the RFX900. The VERT900 antennas support the following frequency bands: 824 to 960MHz, 1710 to 1990MHz with a gain of 3dBi.

The physical dimensions of the E100 mainboard with the RFX900 installed are 158.8mm x 142.9mm X 38.1 (l x w x h).

*a. COM Gumstix Overo*

The embedded computing platform in the E100 is the Gumstix Overo Water COM, based on the ARM Cortex-A8 architecture and a Texas Instruments OMAP 3530 processor. Gumstix markets their COMs as “The world’s smallest Linux computer-on-module” (Gumstix, 2012). Onboard memory is 512MB RAM and storage is provided by a microSD card. Ettus includes a 4GB microSD card with the E100. The entire module measures just 58mm x 17mm x 4.2mm (l x w x h) and weighs 4.3g (Figure 34).



Figure 34. Gumstix Overo COM (From Gumstix, 2012)

The E100 with the installed RFX900 daughter board, SMA cables and Gumstix COM is shown in Figure 35.

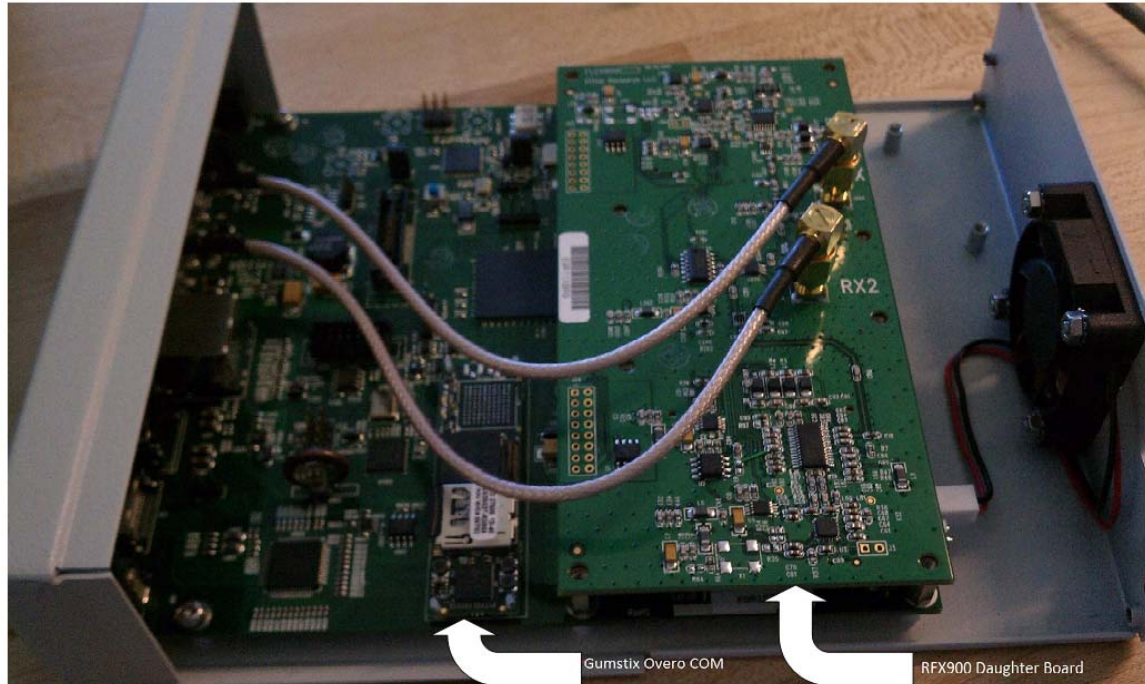


Figure 35. E100 with RFX900 installed

## 2. Test Handsets

In order to test different GSM bands available world-wide, four test handsets and SIM cards were obtained to test with the GSM system. Two handsets were GSM900, one handset was dual band GSM900/850 and one handset was GSM850. All were unlocked from their original network providers (Figure 36). GSM network providers will typically offer mobile handsets at a lower cost to their subscribers. These handsets are obtained from the manufacture at full price which is then subsidized by the GSM network provider. These subsidized handsets are locked to the GSM network provider's network in order to ensure the mobile subscriber continues to pay for service on that specific network. This ensures that the GSM network provider will be able to justify subsidizing the mobile handset. Unlocked handsets have the capability to use any network the subscriber chooses and are usually acquired at a higher price since the devices are not subsidized. Test handsets which are used on a network by a subscriber over a contracted period of time typically can be unlocked from the network at the request of the subscriber or as stipulated in a contract between the subscriber and the network.





Figure 36. Test handsets

## C. SOFTWARE

As previously mentioned the E100 comes with a 4GB microSD card which has a Linux operating system installed along with additional drivers and software. The 4GB microSD card was swapped out with a 16GB microSD card to allow for additional storage. Updated E100 file system images are available through the Ettus website. The current image used for this research is number three, dated 30-March-2012 (Ettus Research LLC, 2012).

### 1. Operating System: Ångström Linux

The Ångström Linux distribution was created by a group of individuals in an effort to provide a stable operating system for embedded devices. It has a package (software) repository which can be accessed by the command line interface (CLI). For a niche Linux distribution it has a fairly extensive package selection which can be browsed

here: <http://www.angstrom-distribution.org/repo/>, however, the package selection is not as robust or up-to-date as more widely-used Linux distributions such as Ubuntu. An attempt was made to install an embedded version of Ubuntu on the COM. This proved to be problematic and time consuming. A root file system had to be built based on Ubuntu and compiled for ARM took up to two hours. A bootable microSD card had to be partitioned and formatted per a developer's guide on the Gumstix website which the author found difficult to follow. Current boot files (separate from the OS) had to be obtained from Gumstix, installed and configured. The guides were followed, but the machine would not fully boot. This was attempted several times before the decision was made to use the file system provided by Ettus. The file system image that came with the E100 already had drivers installed and configured for interfacing with the FPGA and transceiver. GNU Radio.org recommended, "Compiling on the E100 device using the official file system image from Ettus Research is recommended for the majority of users and developers not interested in setting up a cross-compile environment" (GNU Radio, 2011).

## **2. SDR: GNU Radio**

GNU Radio came pre-installed with the E100. GNU Radio is the SDR which the GSM base station software will interface with in order to achieve the desired air interface. With the RFX900 daughterboard installed, a local GSM850 downlink was observed using the GNU Radio graphical user interface (GUI), GNU Radio Companion tuned to 869.5MHz (Figure 37). This showed that the software was interfacing with the hardware properly and the GSM spectrum was being detected accordingly.



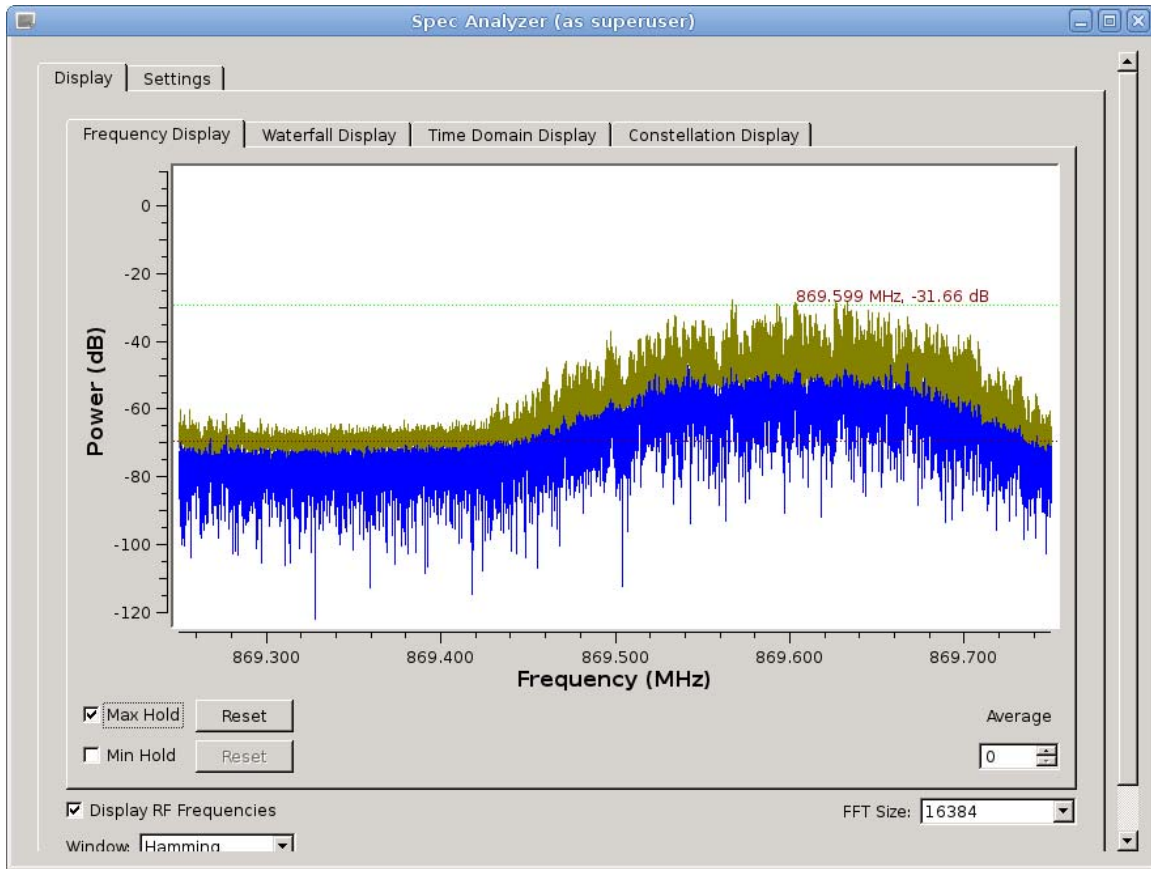


Figure 37. GNU Radio GUI showing GSM850 downlink

### 3. OpenBTS

OpenBTS was a project which started in the summer of 2007, eventually the creators founded Range Networks in late 2010 (Range Networks, 2012). OpenBTS is a Unix open source software application written in C++. OpenBTS interfaces with a SDR to create a GSM air interface. Once the air interface is created, mobile phones can be provisioned and OpenBTS will connect them to a software-based private branch exchange (PBX) which will route calls to a VoIP carrier. OpenBTS is currently available in two different forms: P2.8 which is a free open source software (FOSS) public release and C2.8 which is a commercial release. P2.8 was obtained from RangeNetworks public source code repository. OpenBTS P2.8 is intended for “experimentation, education, evaluation and proof-of-concept projects” (RangeNetworks, 2012).

#### **4. SQLite**

SQLite is an open source standard query language (SQL) database engine. The code for SQLite is in the public domain and free to use for any purpose. It does not use the traditional server-client setup like MySQL. SQLite reads and writes directly to ordinary disk files. Databases for SQLite are created and interacted similar in fashion to the way any other file would be created such as a Word document. SQLite is a relatively small application only using up 358.4kB for a full installation (SQLite, 2012). SQLite is required by the current release of OpenBTS in order to manage mobile users and configuration parameters. A current version of SQLite was available through the Ångström Linux package repository. SQLite can be interacted with using the CLI by merely typing “sqlite3 test.db” which will create a file named: test.db. The CLI can then be used to enter SQL commands to manipulate the new database. There are web browser plugins to interact with SQLite database files and make it easier to view the data contained within.

#### **5. Asterisk VoIP PBX**

Asterisk is an open source private branch exchange (PBX) using VoIP technology. Started, initially, as the Zapata telephony project by Jim Dixon where he conceived that a general purpose CPU would handle DSP functions normally required in telephone systems. General purpose CPUs were much more affordable than DSP chips, so this would lead to a cost-effective telephone solution. A general purpose computer would need nothing more than a circuit card to interface with a telephone system and software could handle the rest (Madsen, Van Meggelen, & Bryant, 2011).

The people behind Asterisk development started a commercial company called Digium in order to offer commercial Asterisk PBX solutions in both software and custom tailored hardware. Digium manages the open source Asterisk community and states, “Asterisk is the world’s most popular open source telephony project” (Digium, Inc., 2012).

Asterisk does not rely on trunks (connections to external networks) and stations (telephone terminal) like a traditional PBX. It instead uses different channels and a

dialplan to manage them. It handles all channels in the same manner regardless of whether the call is internal or external to the network (Madsen, Van Meggelen, & Bryant, 2011).

Asterisk has grown into “a complex system, composed of many resources” (Madsen, Van Meggelen, & Bryant, 2011). In the Ångström Linux OS, the main configuration files are located in the following directory: “/etc/asterisk.” One of the primary files is the “extensions.conf” which makes up the Asterisk dialplan. The Asterisk dialplan is the core of the system which determines how calls are handled (Madsen, Van Meggelen, & Bryant, 2011). Asterisk version 1.4.39.2 was available and installed via the Angstrom software repositories. The current long term support version is 1.8 (Asterisk, 2012).

A common way to manage devices that connect to Asterisk is by using the hardware’s MAC address as a unique identifier. Examples used in “Asterisk: The Definitive Guide” are 000FFFF0001 and 0000FFFF0002. Depending on how a call comes into Asterisk will determine which channel configuration file to use. In the case of VoIP, the channel configuration file that will be is “sip.conf” (session initiation protocol). Once the correct channel configuration file is used, control is passed to the “extensions.conf” which has the information about for handling and routing a call. From Figure 38, the interaction of the “sip.conf” file and the “extensions.conf” can be seen where device with MAC 0000FFFF0001 is dialing extension 101, Asterisk will route the call to the device with MAC 0000FFF0002.

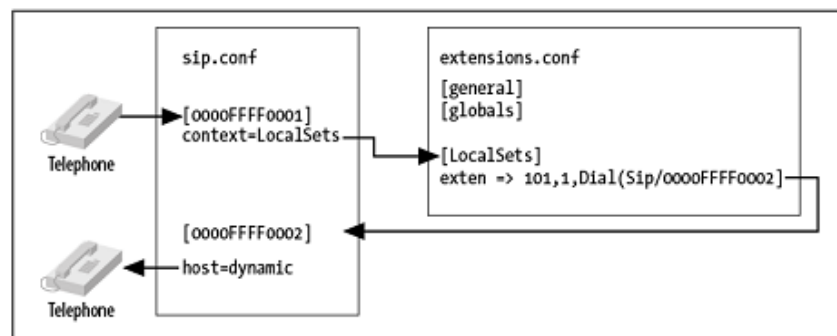


Figure 38. Interaction of “sip.conf” and “extentions.conf” (From Madsen, Van Meggelen, & Bryant, 2011)

Asterisk configuration options are numerous. It can be used to run, monitor and manage a large call center. Calls can be automatically or manually monitored and recorded. Asterisk can route calls differently based on time of day or day of the week. This section was a brief overview on basic setup.

Most interaction and configuration with Asterisk is done through the configuration files or the Asterisk CLI. There have been a number of web-based GUIs developed, and they are available from official sources like Digium or from other open source community projects. Asterisk can be used as a stand-alone system for making calls to different extensions within the network or it can be connected to a VoIP provider which will then enable calls to other PSTN networks.

## 6. System of Software

With the discussion of all the software aside, an overview of how the different software applications interact with each other is shown in Figure 39, where black links are SIP network connections, red links are file system connections (sqlite3 lookups) and blue links are open database connectivity (network/local data base lookups) (Range Networks, 2012) .

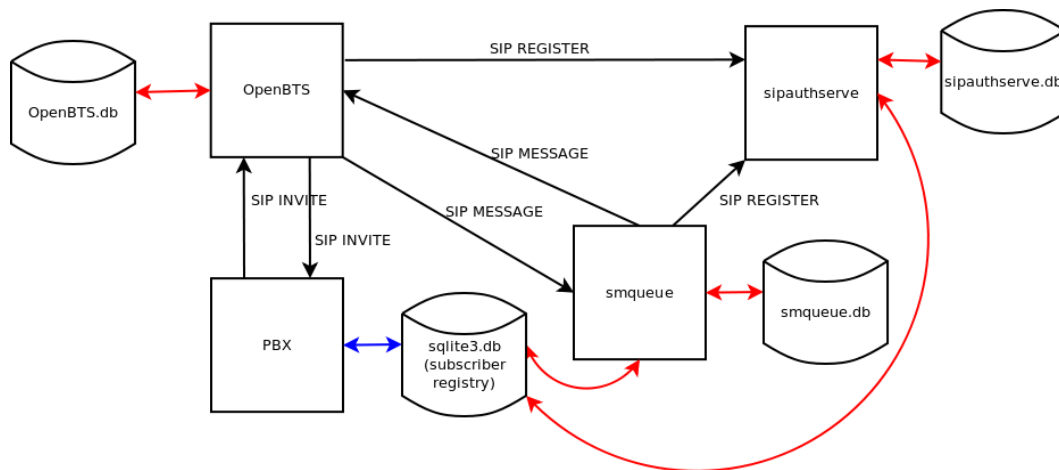


Figure 39. Overview of software interaction (From Range Networks, 2012)

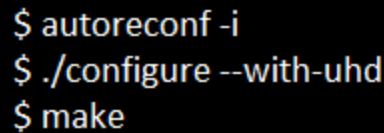
## D. LAB BUILD AND TESTING

### 1. Acquiring OpenBTS

OpenBTS P2.8 was obtained from the Range Networks Public Release source code repository server: <http://wush.net/svn/range/software/public>. The required dependencies, library and utility packages: autoconf, libtool, libosip2, libortp, libusb-1.0, g++, libsqlite3-dev, libboost-all-dev, and libreadline6-dev were all available through the Ångström Linux software repository.

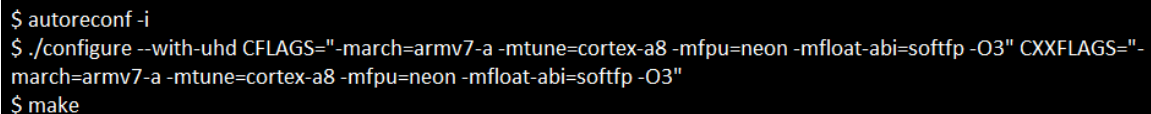
### 2. Build and Install

The guidance for building and installing OpenBTS on the E100 was listed on the Range Networks' site as shown in Figure 40 with configuration for the USRP hardware driver (UHD). On the GNU Radio.org website extra configuration was required specific to optimizing the installation to the Gumstix Overo with ARM7 computing architecture is shown in Figure 41.



```
$ autoreconf -i
$ ./configure --with-uhd
$ make
```

Figure 40. OpenBTS build CLI (From Range Networks, 2012)



```
$ autoreconf -i
$ ./configure --with-uhd CFLAGS="-march=armv7-a -mtune=cortex-a8 -mfloat-abi=softfp -O3" CXXFLAGS="-march=armv7-a -mtune=cortex-a8 -mfloat-abi=softfp -O3"
$ make
```

Figure 41. OpenBTS build CLI specific to ARM processor (From GNU Radio, 2011)

### 3. Configuration

With OpenBTS built, the next step was configuration. This required setting up three different databases shown in Table 11. An application called Smqueue was required to be installed to enable a store-and-forward message service. Smqueue has a database similar to OpenBTS in order to manage configuration and it is found in the following directory: “/etc/OpenBTS/smqueue.db.”

Table 11. OpenBTS Initial Database Setup

Database Name	File Location	Description
OpenBTS.db	/etc/OpenBTS/OpenBTS.db	OpenBTS Configuration
Sqlite3.db	/var/lib/asterisk/sqlite3dir/sqlite3.db	Subscriber Registry
Sipauthserve.db	/etc/OpenBTS/sipauthserve.db	SIP authentication services

#### 4. Initial Run

After the initial configuration of the databases was completed, an attempt was made to run OpenBTS. OpenBTS failed and produced the following error, “TRX clock interface timed out.” Further guidance from GNU Radio.org revealed that an adjustment needed to be made to delay start-up and shutdown of the transceiver. In the OpenBTS.cpp file under the “Start transceiver interface” section, the default sleep value was set at five which needed to be changed to eight (Figure 42).

```
//
// Configure the radio.
//

// Start the transceiver interface.
// Sleep long enough for the USRP to bootload.
sleep(8);
gTRX.start();

// Set up the interface to the radio.
// Get a handle to the C0 transceiver interface.
ARFCNManager* C0radio = gTRX.ARFCN();
```




Figure 42. OpenBTS.cpp TRX sleep value adjustment

With the adjustment made OpenBTS is run along with two other processes (not including Asterisk, which runs at the boot of the Linux OS), smqueue and sipauthserve. Each process requires its own dedicated terminal window. The PuTTY SSH client on a Microsoft Windows computer was used to obtain secure shell access to the E100. Five terminal windows were used to run and monitor the entire system (Figure 43). Windows Secure Copy (WinSCP) program was used to pull database files from the E100 which

were then viewed in a web browser with the SQLite manager plugin. The database files were used to monitor current configuration and data. Configuration of OpenBTS takes place at the OpenBTS CLI (Figure 44). Some parameter changes, such as GSM band adjustment, required a restart of OpenBTS.





The five terminal windows shown in Figure 43 are as follows: 1. OpenBTS CLI, 2. SMQUEUE process, 3. SIPAUTHSERVE process, 4. Asterisk CLI and the system log (SYSLOG) monitor. SYSLOG shows processes associated with OpenBTS such as mobile handsets attaching to the network. It will also show numbers dialed and text messages sent. It will also show a status of a mobile handset detaching from the network.

```
Welcome to OpenBTS. Type "help" to see available commands.

OpenBTS> help

Type "help" followed by the command name for help on that command.

alarms      calls      cellid
chans       config     configsave
endcall     exit       help
load        noise      notices
page        power      regperiod
rxgain      sendsimple  sendsms
tmsis       unconfig   uptime
version

Lines starting with '!' are escaped to the shell.

Use <cntrl-A>, <D> to detach from "screen", *not* <cntrl-C>.

OpenBTS> █
```

Figure 44. OpenBTS CLI

The first settings in OpenBTS were configured for the GSM900 band with an ARFCN of 51 which correlates with an uplink of 900.20MHz and a downlink of 945.20MHz. The cellid parameters were left to default: MCC=001, MNC=01, location area code (LAC)=1000 and cell ID (CI)=10, which correlates with a GSM test network. The “GSM.Identity.ShortName” parameter was set to: NPS, which, depending on the MS, will display as the network carrier. The “Control.LUR.OpenRegistration” was set to non-null in order for non-provisioned handsets (handsets that have not been previously authorized and setup on the network) to attach to the network. All these parameters are managed in OpenBTS.db and can be changed using the CLI for SQLite or by using the

SQLite manager plugin for a web browser. With these parameters in place, two GSM900 handsets registered with the NPS GSM network (Figure 45).



Figure 45. GSM900 test handsets registered to NPS network

## 5. Testing Asterisk Configuration

The IMSIs were easily obtained from the OpenBTS CLI by using the command ‘tmsis’ which displayed the TMSIs and their associated IMSIs for each MS. The MSs also synched and updated to the system time which was set to GMT. The Asterisk sip.conf and extensions.conf files were updated with IMSIs, in place of MAC addresses, for each handset and assigned extension numbers (Table 12).

Table 12. Asterisk parameters

IMSI	Extension
234107330060437	2103
426021823041009	2104

A call was placed from extension 2103 to extension 2104 to test connectivity and the Asterisk dialplan through the system (Figure 46).

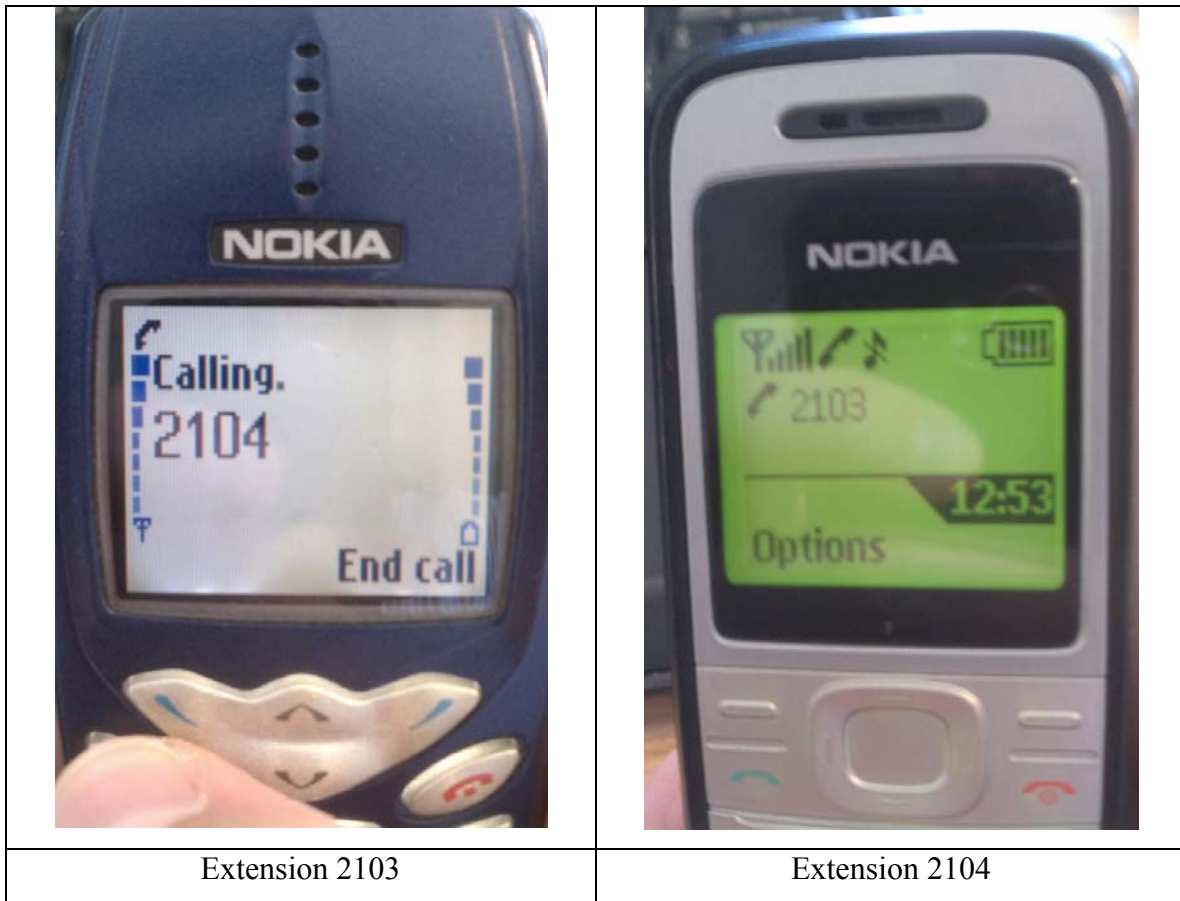
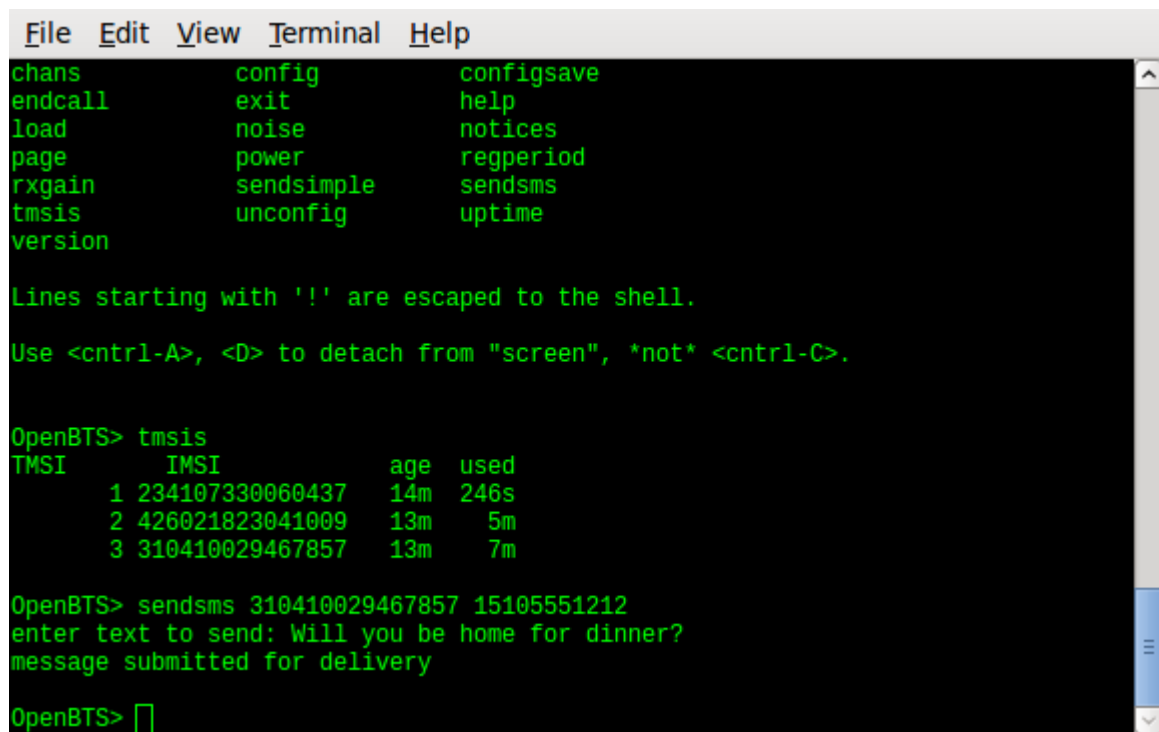


Figure 46. Testing the Asterisk dialplan

One built-in feature with the OpenBTS Asterisk configuration is the echo test. The Asterisk echo test is reached when a handset dials the extension 2600 (extension 600 in standard Asterisk builds), the system will answer and repeat what is spoken into the handset. This allows for checking connectivity over the GSM air interface and to test delay from handset to base station. Sending a null or empty text message (SMS) to extension 411 will have the base station respond with a network status showing that the SMS was received and responded to.

## 6. Testing SENDSMS Function

Using the 'sendsms' command at the OpenBTS CLI allows text messages to be sent to handsets. The 'sendsms' command also allows the OpenBTS operator to choose which phone number the txt is originating from. A notional phone number of (510)555-1212 was obtained from the handset's contacts listing which was listed for the contact "Mother." Text messages could then be sent to the handset which would then appear as they were coming from the contact listed as "Mother." This is illustrated in Figure 47 (text being sent from OpenBTS CLI) and in Figure 48 (handset receiving text).



```
File Edit View Terminal Help
chans          config          configsave
endcall        exit            help
load           noise          notices
page           power          regperiod
rxgain         sendsimple       sendsms
tmsis          unconfig        uptime
version

Lines starting with '!' are escaped to the shell.
Use <cntrl-A>, <D> to detach from "screen", *not* <cntrl-C>.

OpenBTS> tmsis
TMSI      IMSI          age  used
1 234107330060437 14m 246s
2 426021823041009 13m 5m
3 310410029467857 13m 7m

OpenBTS> sendsms 310410029467857 15105551212
enter text to send: Will you be home for dinner?
message submitted for delivery

OpenBTS> 
```

Figure 47. Text message sent via OpenBTS CLI

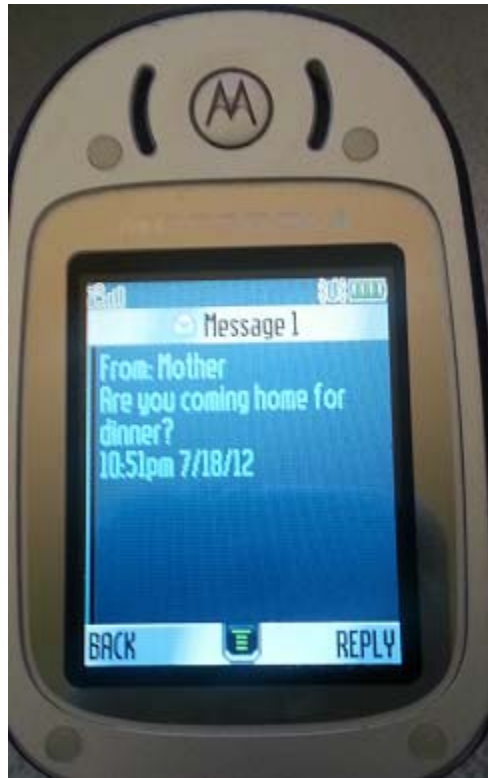


Figure 48. Text message received on handset

## 7. Wi-Fi vs Ethernet Networking

Interacting with the E100 locally required a USB keyboard and mouse. In order to enable wireless networking a USB Wi-Fi adapter was used. For all three USB devices to be connected to the E100, a powered USB hub was required. All these peripheral devices would be unacceptable in achieving a small form factor capable of being mounted in a small UAS. The E100 would not attach to a Wi-Fi network without a user logging in locally to the desktop GUI. The E100 had no problem connecting to a network using the Ethernet connection without user interaction at the local interface. The E100 would boot up and obtain an IP address from either a DHCP server or use a specified IP defined previously, in the network configuration. A user could then access the E100 via SSH. The bare minimum connections required to the E100 for it to function properly as a GSM BTS are power (6V DC/3A) and a network connection via Ethernet and not Wi-Fi.

## 8. Size, Weight and Power

As mentioned previously, the E100 circuit board dimensions are 158.8mm x 142.9mm X 38.1 (l x w x h). While not relatively large, the dimensions are not well suited for a typical small UAS (SUAS) payload compartment.

The majority of the weight of the E100 comes from the metal enclosure. The metal enclosure, screws and fan weigh 953g. The required circuit boards and antennas weigh 291g shown in Figure 48 (without power and networking).



Figure 49. Weight of E100 components

The required system power is 6V DC/3A. The option of using a rechargeable lead-acid battery capable of delivering 6V/4.5Ah was explored. The lead-acid battery was able to power the E100 for just over one hour, however the weight was deemed unacceptable at 724g. To support easier integration into various SUAS configuration a more flexible power solution was researched. Available options included adjustable



power supplies, DC-DC converters and a battery elimination circuit (BEC). All the mentioned options allow for a wide range of DC input voltage levels and then the circuits can be adjusted, either manually or programmed, to meet the required DC voltage output level. In the case of the BEC it is specifically designed to work with lithium-ion polymer (LiPo) batteries which are commonly found in SUAS. It will take an input from 2S to 6S LiPo batteries (5V to 25.2V) and provide a default output of 5.1 volts. The BEC output can be programmed by USB to provide an output between 4.8 and 9 volts (in .1 volt increments), it will support current up to 10A peak and 5A continuous (Castle Creations, 2009).

## **9. Conclusions/Observations**

In order for the E100 OpenBTS to complete outbound phone calls, the Asterisk PBX must be configured to interface with a VoIP provider. There are numerous VoIP providers available with different features, services and pricing available. VoIP providers required an account to be setup and a method to provide payment for services used. Calling extensions within the Asterisk PBS is all handled internally. OpenBTS and Asterisk can be configured to use actual phone numbers for each handset vice using a short extension. Asterisk will treat the phone number as an extension and route the call accordingly.

For calls originating outside of the OpenBTS network to reach a handset inside the network, the VoIP provider must be able to provide direct inward dialing (DID), where a phone number is essentially mapped from the VoIP provider to the Asterisk PBX. Once the phone number reaches the Asterisk PBX, Asterisk must be configured to know what IMSI to forward the inbound call to. Achieving this process in NRT would take extensive system configuration. The phone number assigned to a particular IMSI by a service provider which is then provisioned to the OpenBTS network will not translate from the previous network to the OpenBTS network. For example, if 510-555-1212 is assigned to IMSI 123451234512345 by a specific network provider the handset with that assigned IMSI will be reachable by that phone number on most commercial networks. When IMSI 123451234512345 is provisioned to the OpenBTS network it will no longer

be reachable from outside the network by dialing 510–555–1212. Commercial network providers will be unable to reach the destination handset. In order to overcome this potential limitation, the OpenBTS network operator would have to establish relationships with commercial network providers and negotiate appropriate roaming agreements.

#### **E. INITIAL GROUND TESTING MONTEREY, CA MAY 18, 2012**

Initial ground testing was done to test the E100 BTS outside of the lab to ensure that the system would work on remote power and to test a remote network system to confirm that there would be system connectivity to the Internet. The E100 BTS and supporting network system was vehicle mounted. Network connectivity for the E100 BTS was achieved by using a Linksys router model WRT-54G running custom DD-WRT firmware, which enabled the router to act as a Wi-Fi repeater and access point. Power was supplied by the vehicle's 12VDC power supply. A power inverter was used to convert the 12VDC to 120VAC which was used to power the network components and the E100 BTS (Figure 50).

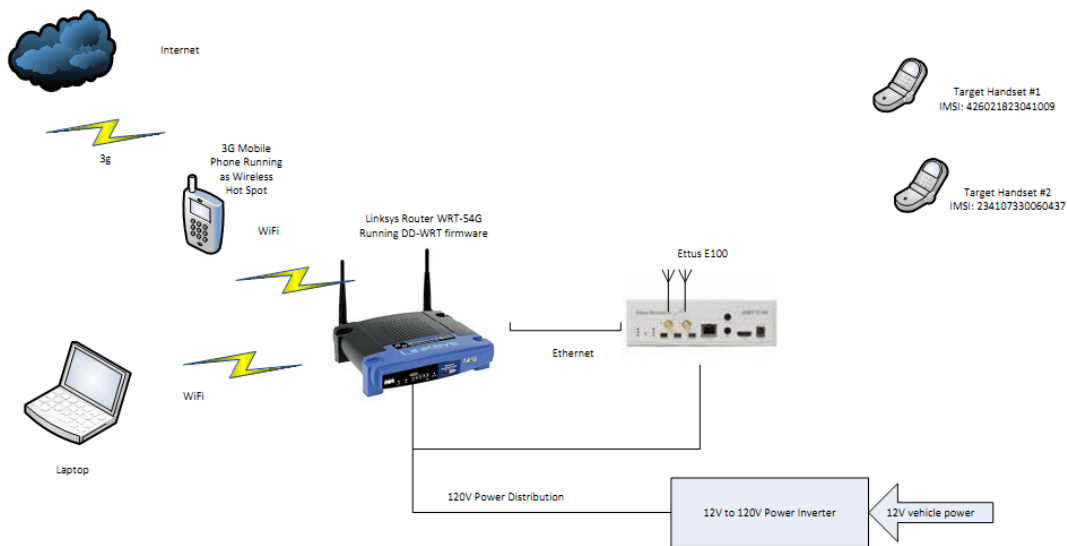


Figure 50. Test network and E100 BTS

The E100 BTS was mounted on top of the vehicle at a height of approximately 2.5m (Figure 51). Two target handsets were powered on and registered with the network.



The target handsets were then moved farther away initially at distances of 10m. The E100 BTS was configured to operate in the GSM900 band with ARFCN of 51. Network connectivity was tested by sending SMS texts (via the 411 extension) to each handset. After 25m, the test handsets were no longer communicating effectively with the E100 BTS. The handsets stayed registered to the network and displayed adequate signal strength out to nearly 100m however, transmit and receive functions were not functional.

The E100 BTS was switched to the GSM850 band with an ARFCN of 180 and a single test handset was used to test connectivity. At a range of 10m, the handset would switch to commercial networks in the area.

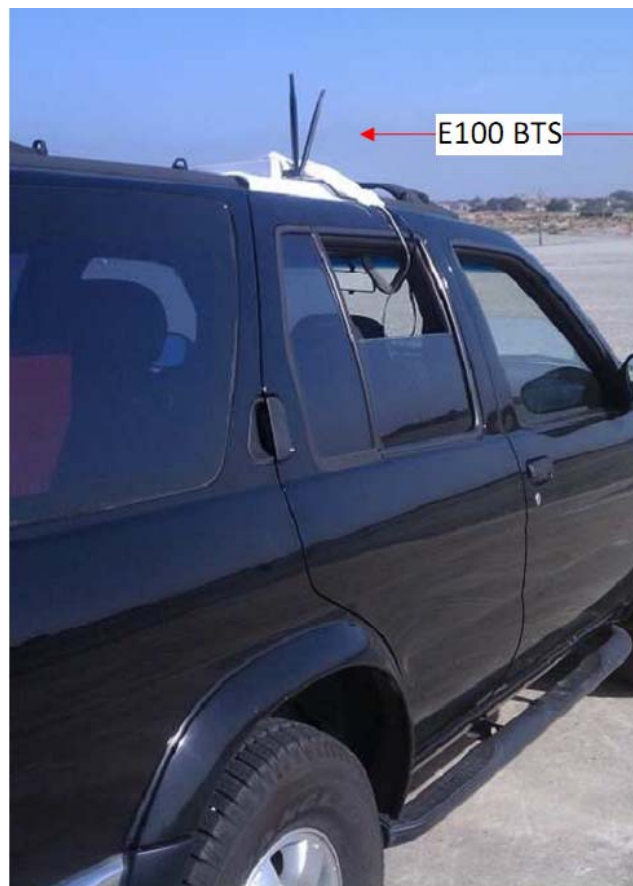


Figure 51. E100 BTS mounted on vehicle

## **1. Conclusions/Observations**

The low effective range was anticipated based on the close proximity of the transmit and receive antennas. This physical configuration created destructive interference between the two antennas. The interfacing with the E100 BTS through the network in Figure 50 was effective with only network and power to the E100.

## **F. CAMP ROBERTS TNT 12-04 TESTING AUGUST 6, 2012**

1. The initial intent was to have the E100 BTS mounted in a small SUAS, but hardware integration was not possible due to time constraints and regulatory issues associated with the FAA/FCC requirements. The E100 BTS was mounted on an available mast at a height of 28'2". Power was supplied by a LiPo battery pack using a battery elimination circuit to achieve the desired voltage required by the E100. A 50' Ethernet cable was used to connect to the WRT-54G router on the ground. The transmit and receive antennas were spaced 24" apart (Figure 52). Testing was done using two target handsets at various ranges. Calls to extension 2600 (echo test) and SMS texts to extension 411 would be used to test effective communication with the E100 BTS. The signal strength indicators on the test handsets would also be observed. A secondary test would be done with the transmit and receive antennas in their stock configuration which is about 3/4" apart.

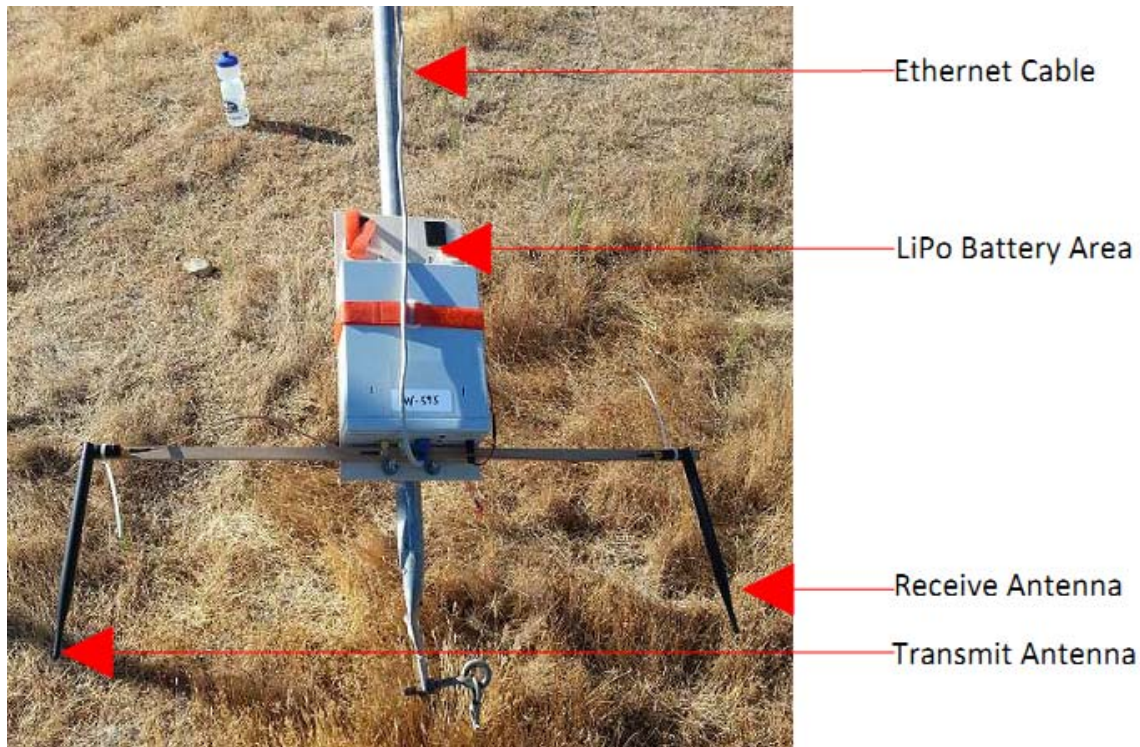


Figure 52. Mast-mounted E100

## 1. Observations

Significant effective communication range improvement was observed. The handsets were able to complete echo test calls and SMS texts out to a range of 260m. Beyond 260m, the handsets were no longer able to register with the network and displayed “no network coverage” errors. The handset test points are labeled A-J and the location of the E100 BTS is labeled “mast” as shown in Figure 53. Specific test results are listed in Table 13. With the transmit and receive antennas placed in their stock positions (3/4” apart) effective communication with the E100 BTS went significantly down to less than 80m. Echo test and a SMS to extension 411 both failed at test point A. The LiPo battery pack effectively powered the E100 BTS for the duration of the testing which was 1hr and 51mins.



Figure 53. Test points A-J around McMillan Airfield

Table 13. Test results at points A-J

Location	Distance from mast (meters)	Results
Mast	0	Test handsets registered to GSM network 'NPS'
A	79	Signal strength excellent, SMS sent/received, echo test passed
B	130	Signal strength good, SMS sent/received, echo test passed
C	153	Signal strength good, SMS sent/received, echo test passed
D	178	Signal strength fair, SMS sent/received, echo test passed
E	205	Signal strength fair, SMS sent/received, echo test failed
F	198	Signal strength fair, SMS sent/received (increase in response time), echo test failed
G	245	Signal strength poor, SMS sent/received, echo test passed
H	505	No network coverage
I	258	Signal strength fair, SMS sent/received (increase in response time), echo test passed
J	378	No network coverage

## **VI. CONCLUSIONS AND RECOMMENDATIONS**

### **A. CONCLUSIONS**

The weight of the core components and the power requirements of the E100 BTS make it a viable candidate to be integrated with a SUAS. The network connectivity requirements would have to be integrated with the SUAS downlink. This added capability will increase the ISR assets at the small unit level. The system could also be used as a potential communications relay or a transparent cell phone jammer where the MS would show great signal strength and connectivity to a GSM network, but no calls or texts could be effectively sent.

While the embedded nature of the E100 allows for development and prototyping of a small form factor GSM base station it certainly has some important limiting factors.

#### **1. Timing Accuracy**

The E100 adjustable TCXO is only accurate to 2.5 parts-per-million (PPM) or  $2.5 \times 10^{-6}$ . While the built-in nature of the E100 TXCO is convenient, it is far from the ETSI GSM Technical Specification max tolerated clock error which is .05ppm ( $5 \times 10^{-8}$ ). This clock discrepancy creates poor synchronization between the MS and the BTS. Call quality can become unacceptable. Ettus Research has a GPS disciplined oscillator (GSPDO) which can be used with the E100 to achieve clock accuracy of .01ppm ( $1 \times 10^{-8}$ ). A clock accuracy of .01ppm is well within the required GSM specifications.

#### **2. RF Isolation**

The E100 is only capable of handling one TX/RX daughter board. Having the TX and RX functions in close proximity to each other causes crosstalk on the two channels. The USRP1 can handle two TX/RX daughter boards, one can handle the TX function and the other can handle the RX function. This separation helps in RF isolation between the TX and RX channels. Separating the TX and RX antennas on the E100 helped in RF isolation, but increased RF isolation would be desired in a production system. Implementation of a duplexer and a low-noise amplified would help isolate the TX and

RX channels. Adding hardware to address the RF isolation issue would, in turn, add weight to the overall system thus complicating the payload restrictions on a SUAS.

### **3. Flexibility**

The attributes of the Gumstix Overo COM offer a small embedded computing solution but this limits the expansion capability, if more computing power is required. The ARM7 computing architecture restricts the use of operating systems to Linux operating systems specifically designed to function on embedded systems. There have been a number of robust small form factor computing platforms that have been made available in recent years, which could be looked at to integrate with one of the Ettus USRP models. Having the computing platform separate from the USRP will allow much more flexibility with regards to system computing architecture.

The RFX900 daughter board is limited to the GSM900 and GSM850 bands. The Ettus Research SBX daughter board covers a wide frequency range, 400–4400MHz, is capable of TX/RX. This would enable a system build which would cover all GSM bands, Wi-Fi, Bluetooth and GPS frequencies. This would allow for a flexible ISR platform to support a wide variety of technologies and mission sets.

### **4. Locked Handheld Devices**

The handheld devices used in this research were all unlocked, meaning that they are free to attach to any GSM network as long as they are compatible with the band. Handheld devices which are not unlocked will only work with a specific network provider. Typically these locked handheld devices were purchased at a reduced price subsidized by the network provider. The handset manufacture designs the device to only work on the GSM networks which the provider has authorized. Authorized networks would include the provider's main network along with any other networks they have established roaming agreements with. Further research would need to be done in this area to figure out how to circumvent this feature.

## **5. Femtocells**

Cellular network service providers in the United States have recently been offering a device called a femtocell or network extenders. A femtocell is used to increase cellular coverage in areas where network coverage may be inadequate or not available at all. These devices connect to an existing broadband Internet connection via an Ethernet cable. Once connected, these devices act as micro cell towers and allow subscribers to connect their mobile handsets to them (Chen, 2010). There are some limitations with the initial configuration and how many devices connect to the femtocell, which could be explored. The technologies femtocells support include GSM, CDMA and 3G.

## **6. Fixed Wing vs VTOL**

Fixed wing SUAS does not offer hovering or perching capabilities which are available in VTOL SUAS. Integrating the E100 GSM system into a VTOL would be ideal so that potential RF fading could be avoided. A VTOL could act as a virtual mast by hovering at a predefined altitude and location. Fixed wing SUAS may be able to achieve a similar objective if it can form a tight loitering circle above a predefined location.

## **7. Concept of Operations (CONOPS)**

Establishing a GSM network where one has been taken down or suppressed would require that the handsets be unlocked in order to use the “new” network. Without an accurate survey of unlocked and locked handsets in a geographic region it would be difficult to assess whether or not most of the mobile subscribers could take advantage of the new network. If most of the handsets in the area were locked, the establishment of a GSM network maybe ineffective.

A backhaul connection to the Internet is necessary if the subscribers attached to the network are able to call outside the network. If the subscribers want to communicate with each other, a connection from the BTS to the Internet is not necessary. If the network is to be completely transparent, work would have to be done with service providers in the region to ensure subscriber phone numbers would be routed to the appropriate handset while on the OpenBTS network.



The limited range of the E100 BTS will allow for precise coverage in a relatively small area. It will not be able to provide broad coverage over a larger area without further enhancements to the hardware.

## **B. RECOMMENDATIONS**

### **1. Technical**

It would be important to find out how well the signal and call quality is improved by first using the GPSDO for correcting the timing of the GSM system. RF isolation could be implemented next. Both of these areas should offer vast improvement and range of the E100 GSM system; however, they will also add overall weight to the system.

### **2. Research**

With an abundance of wireless technologies across a wide variety of protocols and frequencies it would be beneficial to explore the capabilities of using the Ettus SBX daughterboard. This could be used not only in exploiting the wireless technologies, but could be used in jamming them as well.

### **3. Alternative CONOPS**

Use of the GSM BTS in a force protection role could be explored. If a known illicit handset is in the vicinity of friendly forces, it will register with the BTS and the BTS could be configured to send an alert. Seaborne applications could be used whether in supporting a counter piracy role or offering additional shipboard communications capability. This would enable personnel to use their own devices for passing information.

### **4. Adversary Use**

This technology is affordable and available for a wide number of people to obtain and use. It may be worth exploring what potential problems could exist if this was implemented against coalition forces.



## LIST OF REFERENCES

- AeroVironment. (2012, July 26). *Puma AE*. Retrieved from AeroVironment:  
[http://www.avinc.com/uas/small\\_uas/puma/](http://www.avinc.com/uas/small_uas/puma/)
- AeroVironment. (2012, July 28). *Qube*. Retrieved from AeroVironment:  
[http://www.avinc.com/uas/small\\_uas/qube/](http://www.avinc.com/uas/small_uas/qube/)
- AeroVironment. (2012, July 24). *Wasp*. Retrieved from AeroVironment :  
[http://www.avinc.com/uas/small\\_uas/waspAE/](http://www.avinc.com/uas/small_uas/waspAE/)
- Aeryon. (2011, August 23). *Aeryon scout micro UAV helps Libyan rebels in march to Tripoli*. Retrieved from Aeryon: <http://www.aeryon.com/news/pressreleases/271-libyanrebels.html>
- Aeryon. (2012, July 30). *Aerial vehicle systems*. Retrieved from Aeryon:  
<http://www.aeryon.com/products/avs.html>
- Anderson, C. (2012, July). Here come the drones. *Wired Magazine*, 100–111.
- ArduCopter. (2012, July 27). *ArduCopter Wiki*. Retrieved August, 7, 2012, from ArduCopter: <http://code.google.com/p/arducopter/wiki/ArduCopter>
- Asterisk. (2012, August 8). *Asterisk versions*. Retrieved from Asterisk:  
<https://wiki.asterisk.org/wiki/display/AST/Asterisk+Versions>
- Bacon, L. M. (2011, November 13). *Soldiers rate the best new combat gear*. Retrieved from *Army Times*: <http://www.armytimes.com/news/2011/11/army-soldiers-rate-best-new-gear-111311w/>
- Bannister, J., Mather, P., & Coope, S. (2004). *Convergence technologies for 3G networks: IP, UMTS, EGPRS and ATM*. West Sussex: John Wiley & Sons, Ltd.
- Bonsor, W. (1998). *International Symposium on Advanced Radio Technologies 1998*. Retrieved 2012, from Institute for Telecommunication Sciences Boulder, Colorado: [http://www.its.bldrdoc.gov/isart/art98/slides98/bons/bons\\_s.pdf](http://www.its.bldrdoc.gov/isart/art98/slides98/bons/bons_s.pdf)
- Bort, J. (2010, August 30). *Burning Man's open source cell phone system could help save the world*. Retrieved 2012, Network World:  
<http://www.networkworld.com/news/2010/083010-open-source-voip-cell-phones-at-burning-man.html>

- Business Wire. (2011, August 30). *AeroVironment Introduces Shrike Vertical Take-off and Landing (VTOL) Unmanned Aircraft System*. Retrieved from Business Wire:  
<http://www.businesswire.com/news/home/20110830006032/en/AeroVironment-Introduces-Shrike-Vertical-Take-off-Landing-VTOL>
- Castle Creations. (2009, June 15). *Castle Creations BEC User Guide*. Retrieved from Castle Creations:  
[http://www.castlecreations.com/support/documents/cc\\_bec\\_user\\_guide.pdf](http://www.castlecreations.com/support/documents/cc_bec_user_guide.pdf)
- Chen, B. X. (2010, March 24). *With AT&T Femtocell, Your Coverage Troubles Could Be Over*. Retrieved from Wired: <http://www.wired.com/gadgetlab/2010/03/att-microcell/>
- Congressional Budget Office. (2011). *Policy options for unmanned aircraft systems*. Washington, DC: Congress of the United States.
- Department of Defense. (2009). *Office of the Secretary of Defense unmanned systems integrated roadmap*. Washington, DC: Department of Defense.
- Digium, Inc. (2012, August 3). *About digium*. Retrieved from Digium:  
<http://www.digium.com/en/company/>
- Dillow, C. (2011, July 29). *DIY UAV That Hacks Wi-Fi Networks, Cracks Passwords, and Poses as a Cell Phone Tower*. *Popular Science*.
- DIY Drones. (2012, July 25). *ArduCopter 3DR-B Frame + Motors + Full Flight electronics kit*. Retrieved from DIY Drones:  
[https://store.diydrones.com/Arducopter\\_3DR\\_B\\_Electronics\\_Kit\\_p/kt-ac3dr-03.htm](https://store.diydrones.com/Arducopter_3DR_B_Electronics_Kit_p/kt-ac3dr-03.htm)
- Eged, B., & Babjak, B. (2006). *Universal software defined radio development platform*. Budapest: Sagax Communications Ltd. Retrieved July 22, 2012
- E-Sytems. (1985, May). *New Research Lab Leads to Unique Radio Receiver*. *E-Sytems TEAM*, 5(4), pp. 6–7.
- Ettus Research, LLC. (n.d.). *Ettus Research Daughterboards*. Retrieved July 23, 2012, from Ettus Research website:  
<https://www.ettus.com/product/category/Daughterboards>
- Ettus Research LLC. (2012, July 23). *Ettus USRP E100 product description*. Retrieved from Ettus Research : [https://www.ettus.com/content/files/Ettus\\_E100-110\\_DS\\_FINAL\\_1.27.12.pdf](https://www.ettus.com/content/files/Ettus_E100-110_DS_FINAL_1.27.12.pdf)

- Ettus Research LLC. (2012, August 2). *Elxx images*. retrieved from ettus research, llc: [http://files.ettus.com/elxx\\_images/](http://files.ettus.com/elxx_images/)
- Garcia, R. D., & Valavanis, K. P. (2007). A Modular On-board Processing System for Small Unmanned Vehicles. In K. P. Valavanis, *Advances in Unmanned Aerial Vehicles* (pp. 495–529). Dordrecht: Springer.
- Global Mobile Suppliers Association. (2010). *GSM/3G stats*. Retrieved July 23, 2012, from Global Mobile Suppliers Association: <http://www.gsacom.com/news/statistics.php4>
- GNU Radio. (2011, May 26). *OpenBTS: USRP E100*. Retrieved from GNURadio.org 05/26/2011: <http://gnuradio.org/redmine/projects/gnuradio/wiki/OpenBTSE100>
- GNU Radio. (2012, July 23). *GNURadio.org home page*. Retrieved from GNU Radio: <http://gnuradio.org/redmine/>
- Gumstix. (2012, August 2). *Gumstix overo COMS Open Source Products*. Retrieved from Gumstix: <https://www.gumstix.com/store/index.php?cPath=33>
- jDrones. (2012, August 28). *ArduCopter quad v1.1 KIT*. Retrieved from jDrones: [http://store.jdrones.com/product\\_p/ackit1sol.htm](http://store.jdrones.com/product_p/ackit1sol.htm)
- Lawson, S. (2008, February 14th). *Most analog cellular to fade away on Monday*. Retrieved from InfoWorld: <http://www.infoworld.com/t/communication-and-collaboration/most-analog-cellular-fade-away-monday-423>
- Lockheed-Martin. (2012, January 17). *Lockheed Martin acquires procerus technologies*. Retrieved from Lockheed-Martin: <http://www.lockheedmartin.com/us/news/press-releases/2012/january/0117hq-procerus.html>
- Lockheed-Martin. (2012, July 25). *Desert Hawk III*. Retrieved from Lockheed Martin: [http://www.lockheedmartin.com/content/dam/lockheed/data/ms2/documents/Desert\\_Hawk\\_III\\_brochure.pdf](http://www.lockheedmartin.com/content/dam/lockheed/data/ms2/documents/Desert_Hawk_III_brochure.pdf)
- Lockheed-Martin. (2012, July 23). *Stalker UAS*. Retrieved from Lockheed-Martin: <http://www.lockheedmartin.com/us/products/stalker-uas.html>
- Madsen, L., Van Meggelen, J., & Bryant, R. (2011). *Asterisk: The Definitive Guide* (3rd ed.). Sebastopol: O'Reilly Media.
- MCCLIST. (2012, July 23). *Mobile country codes (MCC) and Mobile Network Codes (MNC)*. Retrieved from MCCLIST: <http://mobile-network-codes.com/mobile-network-codes-country-codes.asp>

- Messmer, E. (2011, January 19). *Fake GSM base station trick targets iPhones*. Retrieved from Network World: <http://www.networkworld.com/news/2011/011911-black-hat-trick-iphones.html>
- Nathans, D., & Stephens, D. (2007). Reconfiguring to Meet Demands: Software Defined Radio. *CrossTalk: The Journal of Defense Software Engineering*, 24–27. Retrieved July 23, 2012, from <http://www.crosstalkonline.org/storage/issue-archives/2007/200707/200707-0-Issue.pdf>
- Naughton, D. R. (2005, July 24). *Remote piloted aerial vehicles - The Northrop radioplane target drone*. Retrieved from Monash University: [http://www.ctie.monash.edu.au/hargrave/rpav\\_radioplane6.html](http://www.ctie.monash.edu.au/hargrave/rpav_radioplane6.html)
- Noldus, R. (2006). *CAMEL: Intelligent networks for GSM, GPRS and UMTS network*. West Sussex: John Wiley & Sons, Ltd.
- Range Networks. (2012, July 8). *Building, installing and running OpenBTS*. Retrieved from RangeNetworks OpenBTS Public Release: <http://wush.net/trac/rangepublic/wiki/BuildInstallRun>
- Range Networks. (2012, August 2). *About*. Retrieved from RangeNetworks: <http://www.rangenetworks.com/about/>
- RangeNetworks. (2012, August 3). *OpenBTS Public Release*. Retrieved from RangeNetworks Public Trac: <http://wush.net/trac/rangepublic>
- Reed, J. (2002). *Software Radio: A modern approach to radio engineering*. Upper Saddle River: Prentice Hall.
- Rubin, A. J. (2011, October 4). *Taliban using modern means to add to sway*. Retrieved from The New York Times: [http://www.nytimes.com/2011/10/05/world/asia/taliban-using-modern-means-to-add-to-sway.html?\\_r=2&pagewanted=all](http://www.nytimes.com/2011/10/05/world/asia/taliban-using-modern-means-to-add-to-sway.html?_r=2&pagewanted=all)
- Sauter, M. (2011). *From GSM to LTE: An introduction to mobile networks and mobile broadband*. West Sussex: John Wiley & Sons, Ltd.
- Schaefer School of Engineering & Science. (2010, November 19). *Dr. Joseph Mitola presents future of wireless at IEEE GLOBECOM 2010*. Retrieved July 24, 2012, from Stevens Institute of Technology: <http://buzz.stevens.edu/index.php/mitola-ieee-globecom-wireless>
- Sklar, B. (2001). *Digital Communication: Fundamentals and Applications* (2nd ed.). New Jersey: Prentice Hall.
- Spareone. (2012). *GSM Map*. Retrieved from Spareone: <http://spareone.com/gsm-map/>

- Spicer, Alan. (2010). *OpenBTS: An opensource telephone network*. Retrieved from Alan Spicer Marine Telecom Blog:  
<http://blog.marinetelecom.net/2010/08/01/openbts-an-opensource-telephone-network-alans-additional-note-an-opensource-gsm-cellular-telephone-network/>
- SQLite. (2012, August 2). *About SQLite*. Retrieved from SQLite:  
<http://www.sqlite.org/about.html>
- Stallings, W. (2005). *Wireless communications & networks* (2nd ed.). Upper Saddle River, New Jersey: Pearson Prentice Hall.
- Telecom ABC. (2005). *ARFCN*. Retrieved from Telecom ABC:  
<http://www.telecomabc.com/a/arfcn.html>
- U.S. Army. (2010). *U.S. Army unmanned aircraft systems roadmap 2010–2035*. Fort Rucker: U.S. Army UAS Center of Excellence.
- U.S. Department of Transportation Federal Aviation Administration. (2008). *Pilot's Handbook of Aeronautical Knowledge FAA-H8083–25A*. Oklahoma City: United States Department of Transportation, Federal Aviation Administration.
- U.S. Air Force. (2011, September 14). *Wasp III Fact Sheet*. Retrieved from USAF:  
<http://www.af.mil/information/factsheets/factsheet.asp?id=10469>
- U.S. Air Force. (2012, Jan 27). *Factsheets: RQ-4 Global Hawk*. Retrieved from USAF:  
<http://www.af.mil/information/factsheets/factsheet.asp?id=13225>
- Valerio, D. (2008). *Open source software-defined radio: A survey on GNURadio and its applications*. Vienna: Telecommunications Research Center Vienna (FTW).
- Warwick, G. (2012, May 25). *AeroVironment, Textron Advance Lethal Mini-UASs*. Retrieved from Aviation Week:  
[http://www.aviationweek.com/Article/PrintArticle.aspx?id=/article-xml/asd\\_05\\_25\\_2012\\_p02-01-461914.xml&p=1&printView=true](http://www.aviationweek.com/Article/PrintArticle.aspx?id=/article-xml/asd_05_25_2012_p02-01-461914.xml&p=1&printView=true)
- Wireless Innovation Forum. (2012, July 22). *Introduction to SDR*. Retrieved July 24, 2012, from Wireless Innovation Forum:  
[http://www.wirelessinnovation.org/Introduction\\_to\\_SDR](http://www.wirelessinnovation.org/Introduction_to_SDR)
- Zaloga, S. J. (2008). *Unmanned aerial vehicles*. New York: Osprey Publishing Ltd.

THIS PAGE INTENTIONALLY LEFT BLANK

## INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center  
Ft. Belvoir, Virginia
2. Dudley Knox Library  
Naval Postgraduate School  
Monterey, California
3. Dr. Dan C. Boger  
Chairman  
Code IS Department of Information Sciences  
Naval Postgraduate School  
Monterey, California
4. Dr. Raymond R. Buettner  
Associate Professor  
Department of Information Sciences  
Naval Postgraduate School  
Monterey, California
5. Dr. Kevin D. Jones  
Research Associate Professor  
Department of Mechanical and Aerospace Engineering  
Naval Postgraduate School  
Monterey, California